GUÍA DE USUARIO

Bitdefender CONSUMER SOLUTIONS

Security for Creators

Bitdefender Security for Creators

Guía de usuario

Fecha de publicación 07/04/2023

Aviso Legal

Bitdefender

Tabla de contenidos

ACERCA DE ESTA GUÍA

Propósito y público al que se dirige

Esta guía proporciona ayuda para la configuración y el uso de los productos de su suscripción, diseñada específicamente para creadores de contenidos como usted: Bitdefender Security for Creators.

Podrá aprender a configurar Bitdefender en diferentes dispositivos para mantenerlos a salvo de todo tipo de amenazas y, lo que es más importante, descubrirá cómo proteger su cuenta de YouTube frente a cualquier ataque informático directo o intento de piratería.

Cómo usar esta guía

Esta guía aborda los cuatro productos incluidos en el paquete **Bitdefender Security for Creators**:

- Security for Creators (página 4)
  Descubra cómo usar Security for Creators para proteger y monitorizar mejor su canal de YouTube, con el fin de prevenir cualquier posible apropiación de su cuenta o sabotaje de sus contenidos.
- Email Protection
  Aprenda a proteger mejor su bandeja de entrada de correo electrónico contra el spam, los correos electrónicos maliciosos y los intentos de phishing gracias a Email Protection.
- Seguridad Total para PC (página 16)
  Aprenda a usar el producto en sus PC y portátiles Windows.
- Antivirus para Mac (página 159)
  Aprenda a usar el producto en sus Macs.
- Seguridad móvil para Android (página 192)
  Aprenda a usar el producto en sus tablets y smartphones Android.
- Seguridad móvil para iOS (página 226)
  Aprenda a usar el producto en sus tablets y smartphones iOS.
- vpn (página 241)
  Aprenda a ocultar su identidad online usando Bitdefender VPN en cualquiera de sus dispositivos.

Convenciones utilizadas en esta guía

Convenciones tipográficas

En esta guía se utilizan distintos estilos de texto con el fin de mejorar su lectura. En la siguiente tabla se indican su aspecto y significado.

Apariencia	Descripción
sample syntax	Las muestras de sintaxis se imprimen con monospaced caracteres.
https://www.bitdefender.com	La URL del enlace señala a alguna ubicación externa, en servidores http o ftp.
documentation@bitdefender.com	Las direcciones de email se incluyen en el texto como información de contacto.
Acerca de esta guía (página 1)	Este es un enlace interno, hacia algún punto dentro del documento.
filename	Los archivos y directorios se imprimen usando monospaced fuente.
opción	Todas las opciones de productos se imprimen usando **atrevido** caracteres.
palabra clave	Las palabras clave o frases importantes se resaltan usando **atrevido** caracteres.

Advertencias

Las advertencias son notas en el texto, marcadas gráficamente, que brindan información adicional respecto al párrafo actual.

Nota

La nota es una pequeña observación. Aunque puede omitirla, las notas pueden proporcionar información valiosa, como características específicas o enlaces hacia temas relacionados.

Importante

Este tipo de advertencia requiere su atención y no es recomendable omitirla. Normalmente proporciona información importante, aunque no extremadamente crítica.

Advertencia

Se trata de información crítica que debería tratar con extrema cautela. No ocurrirá nada malo si sigue las indicaciones. Debería leer y entender estas notas, porque describen algo extremadamente arriesgado.

Solicitud de comentarios

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

Háganos saber enviando un correo electrónico a documentation@bitdefender.com. Escriba todos sus correos electrónicos relacionados con la documentación en inglés para que podamos procesarlos de manera eficiente.

1. SECURITY FOR CREATORS

1.1. Qué es Bitdefender Security for Creators

Bitdefender Security for Creators es la solución de seguridad informática de Bitdefender diseñada para proteger a los creadores de contenidos, independientemente de las características de su canal y del número de suscriptores que tengan. Incluye lo siguiente:

- **Protección del canal de YouTube:** Monitoriza en todo momento su canal de YouTube para detectar cualquier intento de apropiación de su cuenta y le proporciona una sencilla guía de recuperación paso a paso en caso de que esta resulte pirateada.
- **Protección de dispositivos:** La aplicación de seguridad de Bitdefender protege todos sus dispositivos, salvaguarda sus credenciales de inicio de sesión y el uso de redes Wi-Fi públicas, marca los correos electrónicos de falsos patrocinadores, etc.

> **Nota**
> Actualmente, Security for Creators únicamente monitoriza y protege las cuentas de YouTube, pero estamos trabajando para ampliar nuestra cobertura a las principales plataformas que usan actualmente los creadores de contenidos.

A diario, se piratean canales de YouTube para realizar falsas transmisiones en directo, promover estafas, como obsequios de criptomonedas, o exigir el pago de un rescate. Bitdefender Security for Creators es todo lo que los creadores de contenidos necesitan para mantener a salvo su cuenta de YouTube. Ayuda a la recuperación rápida de las cuentas en caso de que resulten pirateadas y notifica al usuario de cualquier cambio sospechoso realizado en el canal, como la eliminación de varios vídeos en un corto período de tiempo o la rápida modificación de las imágenes del perfil o banner, de las descripciones y de otros componentes del canal de YouTube, lo cual es un típico síntoma de la apropiación de su cuenta.

1.2. Configuración de Security for Creators

Para configurar su suscripción de Bitdefender Security for Creators, lo primero es activar el producto para poner en marcha el proceso:

- **Activar la solución:** Inmediatamente después de realizar la compra, debería recibir un correo electrónico en su bandeja de entrada. Siga las instrucciones del mensaje de confirmación para activar su suscripción a Bitdefender Security for Creators.

Una vez hecho esto, es el momento de configurar su plan de Bitdefender:

1. En la pantalla que confirma la activación de su suscripción, haga clic en el botón **Puesta en marcha** para dar comienzo a la configuración. Como alternativa, en caso de que haya abandonado esa ventana, haga clic en **Security for Creators** en el menú de la izquierda de su cuenta de Bitdefender.
2. Haga clic en el botón **Comencemos** para llevar a cabo un proceso de configuración rápida.
3. Conecte su canal de YouTube de la siguiente manera:
   a. Haga clic en el botón **Iniciar sesión con Google**.
   b. Utilice la cuenta de Google vinculada a su canal de YouTube. Introduzca su contraseña y compruebe su número de teléfono en caso de que se le solicite. Luego, haga clic en **Siguiente**.
   c. Haga clic en **Continuar** para otorgar los permisos necesarios y que Bitdefender pueda proteger su canal de YouTube.
4. Proteja su dispositivo. Descargue e instale la aplicación de Bitdefender para atajar cualquier amenaza a la que pueda verse expuesto su dispositivo.
   a. Haga clic en el botón **Descargar**.
   b. Siga las instrucciones que aparecen en la pantalla para instalar la aplicación Bitdefender en su dispositivo.
   c. Una vez instalado, haga clic en **Siguiente** para continuar.
5. **Finalizar la configuración:** Haga clic en el botón **Pasar a su panel de control** para abrir su panel de Bitdefender Central.

¡El proceso de incorporación ha finalizado!

1.3. Características y funcionalidades

Puede acceder al panel de control de Security for Creators desde el menú izquierdo de su cuenta de Bitdefender.

Desde aquí, puede proteger y recuperar fácilmente su canal de YouTube, gestionar el acceso del equipo y monitorizar la actividad, lo que garantiza un entorno más seguro y productivo para su trabajo creativo. A continuación, detallamos las características y funcionalidades de Bitdefender Security for Creators.

1.3.1. Actividad

Detalles del canal:

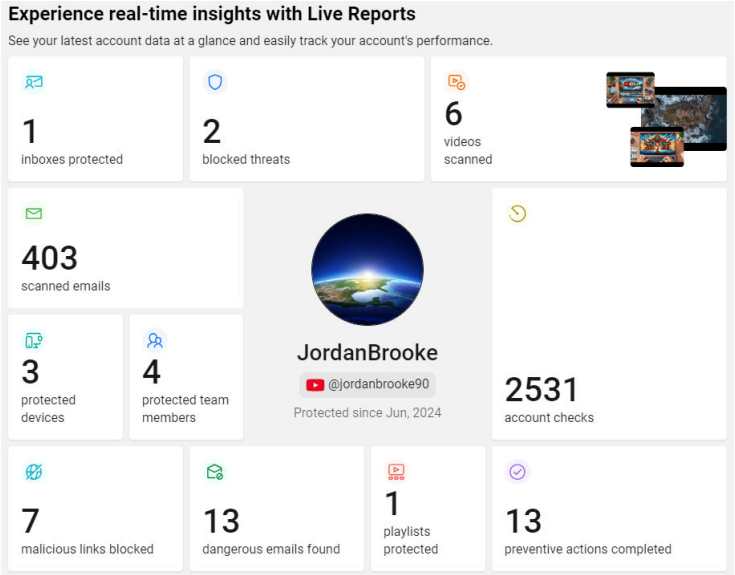
En la parte superior de la pestaña Actividad, hallará toda la información básica relativa a su canal de YouTube.

- Foto del perfil y nombre del canal
- Número de suscriptores y número de vídeos cargados actualmente.

Informes en directo:

El botón de Informes en directo brinda análisis y valiosa información en tiempo real sobre la seguridad de su canal, lo que incluye lo siguiente:

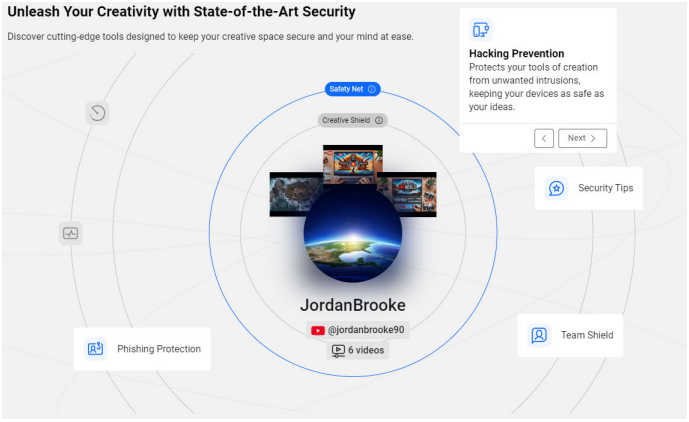
- Número de dispositivos y miembros del equipo monitorizados y protegidos, bandejas de entrada monitorizadas.
- Número de mensajes de correo electrónico peligrosos y URL maliciosas que se han bloqueado.
- Número de mensajes de correo electrónico y vídeos analizados, así como el número de comprobaciones de la cuenta realizadas por Bitdefender.



Tecnologías:

Las tecnologías facilitan la exploración de todas las características de Bitdefender Security for Creators.

Pulse el botón **Siguiente** o haga clic en cualquier característica para obtener más información:



Valiosa información de seguridad en tiempo real:

Desplazándose hacia abajo en la página de Actividad accede a la siguiente información:

- **Actividad del canal de YouTube:** Información actualizada sobre las actividades recientes de su canal.
- **Recomendaciones de seguridad:** Consejos sobre seguridad para que mantenga su cuenta a salvo de los piratas informáticos. Por cada recomendación de seguridad (por ejemplo: 'Revisar las apps de terceros' o 'Revisar las opciones de recuperación'), haga clic en el botón **Revisar**. Así, se le conducirá a una página donde podrá revisar o eliminar los elementos según corresponda.
  Tras aplicar las acciones recomendadas, haga clic en el botón **Marcar como hecho**.
- **Alertas críticas y orientación para la recuperación:** En caso de que se detecten actividades sospechosas (por ejemplo, la eliminación de varios vídeos o la transmisión y cambios inusuales en los contenidos), la pestaña **Actividad** emitirá alertas críticas. Dicha alertas le guiarán paso a paso por las acciones necesarias para recuperar y proteger rápidamente su canal de YouTube contra futuros ataques de piratería informática.

1.3.2. Seguridad

Desde la pestaña **Seguridad**, puede comprobar rápidamente su seguridad y ver sus dispositivos y su correo electrónico protegidos, así como las amenazas bloqueadas en el pasado. La pestaña **Seguridad** se divide en dos secciones: **Mis dispositivos** y **Email Protection**.

- **Mis dispositivos**
  - Proteja nuevos dispositivos Windows, macOS, iOS y Android.
  - Vea un resumen de las amenazas para la seguridad informática detectadas recientemente.
  - Vea los dispositivos protegidos actualmente por Bitdefender.
- **Email Protection**
  - Vea el total de mensajes de correo electrónico analizados por Bitdefender Email Protection durante los últimos treinta días, desglosados en mensajes seguros y peligrosos.

- Vea todos los buzones protegidos y su estado actual.

1.3.3. Miembros del equipo

La pestaña **Miembros del equipo** le permite gestionar a los miembros del equipo de su canal de YouTube:

- Envíe invitaciones por correo electrónico para proteger a nuevos miembros del equipo.
- Elimine a miembros actuales del equipo.

1.4. Eliminar y añadir un canal de YouTube distinto

Para eliminar un canal de YouTube monitorizado y configurar una cuenta diferente en Bitdefender Security for Creators, ha de seguir las instrucciones que figuran a continuación:

1.4.1. Eliminar un canal de YouTube monitorizado

1. Inicie sesión en su cuenta de Bitdefender Central.
2. Una vez que haya iniciado sesión, haga clic en su nombre de usuario o en el icono del perfil ubicado en la esquina superior derecha de la página.
3. En el menú, seleccione **Ajustes**. Se abrirá la página de ajustes de la cuenta de Bitdefender.
4. En la sección **Administrar cuentas**, haga clic en **Eliminar cuenta**.
5. Aparecerá una ventana emergente solicitándole que confirme la eliminación del canal.
   Haga clic en **Eliminar cuenta** para confirmar la acción.

   Importante
   Cuando Bitdefender Security for Creators deje de monitorizar un canal de YouTube, no recibirá ninguna alerta en caso de que un pirata informático tome el control de esa cuenta.

1.4.2. Añadir un canal de YouTube distinto

1. Acceda a los ajustes de su cuenta:

- Si acaba de eliminar una cuenta de YouTube, verá un botón **Conectar su cuenta** en la sección **Administrar cuentas**.
- En caso de que esté empezando desde cero, inicie sesión en su cuenta de Bitdefender Central, haga clic en su nombre de usuario o en el icono del perfil y seleccione **Ajustes** en el menú.

2. Haga clic en el botón **Conectar su cuenta** de la sección **Administrar cuentas**.
3. Se le conducirá al panel de control de Bitdefender Security for Creators.
   Desplácese hacia abajo y haga clic en el botón **Reconectar** del panel **Canal de YouTube desconectado**.
4. Una ventana emergente le solicitará que conecte su cuenta de YouTube. Haga clic en el botón **Iniciar sesión con Google**.
5. Elija la cuenta de Google correspondiente al canal de YouTube que desee monitorizar.
   Introduzca su contraseña, en caso de que se le solicite, y, a continuación, haga clic en **Siguiente**.
6. Haga clic en **Continuar** para permitir que Bitdefender Security for Creators proteja su cuenta de YouTube.

Una vez establecida correctamente la conexión, el nombre y la foto del perfil del canal de YouTube vinculado aparecerán en la parte superior del panel de control de Bitdefender Security for Creators.

1.5. Recuperar una cuenta de YouTube pirateada

Para recuperar el control de su cuenta y protegerla contra futuros ataques similares es crucial que actúe inmediatamente. Con Bitdefender Security for Creators, recuperar un canal de YouTube pirateado es un proceso sencillo y guiado paso a paso.

Esto es lo que debe hacer si su canal de YouTube resultase pirateado:

Paso 1: Abra el correo electrónico de Bitdefender que acaba de recibir

En cuanto su canal de YouTube sea pirateado, recibirá por correo electrónico una alerta de Bitdefender titulada **Actividad sospechosa detectada**. Dicho mensaje se envía a la dirección de correo electrónico que haya utilizado para crear su cuenta de Bitdefender Central y

contiene información sobre todas las actividades sospechosas y acciones reseñables que se han detectado en el canal, como:

- Porcentaje de vídeos eliminados (por ejemplo: se ha eliminado el 55 % de los vídeos).
- Cambios en el banner, las miniaturas de los vídeos, la foto del perfil y la descripción del canal.

Haga clic en el botón **Proteger su cuenta ahora** que aparece en el correo electrónico.

Paso 2: ¿Qué ha sucedido?

Esto le conducirá a su cuenta de Bitdefender Central, donde una ventana emergente le informará de que su canal de YouTube se ha visto comprometido.

En la sección **Ver qué ha pasado**, hallará (y podrá volver a consultar) una lista detallada de todos los cambios detectados en su cuenta de YouTube.

Paso 3: Recuperar un canal de YouTube pirateado en cuatro pasos

1. **Acceder a su cuenta:** Acceda a los enlaces del menú **Acceder a su cuenta** para recuperar rápidamente su cuenta. Si no pudiera iniciar sesión, póngase en contacto enseguida con el servicio de soporte técnico de YouTube a través de los enlaces proporcionados.
2. **Restablecer su contraseña:** Haga clic en el enlace del menú **Restablecer su contraseña** para establecer una contraseña segura y única de al menos ocho caracteres que incluya letras mayúsculas y minúsculas, números y caracteres especiales.
3. **Revisar sus ajustes:** Acceda a los enlaces para eliminar a cualquier miembro del equipo que no le sea conocido, dispositivos no autorizados y aplicaciones de terceros que resulten sospechosas.
4. **Comprobar su información de recuperación:** Cerciórese de que su información de recuperación sea correcta para evitar futuros accesos no autorizados.

Recuerde que si han utilizado su cuenta para publicar contenidos inapropiados o si han eliminado vídeos, debería comunicárselo a su público. Publique un vídeo o un aviso a la comunidad explicando la situación y las medidas que ha adoptado para resolverla. Este ejercicio de transparencia puede contribuir a mantener la confianza y el apoyo de sus suscriptores.

1.6. Preguntas frecuentes

¿Cómo me ayuda Bitdefender en caso de que mi canal de YouTube resulte pirateado?

Si alguien piratea su canal de YouTube, Bitdefender le enviará una alerta por correo electrónico con una guía paso a paso y enlaces directos a Google/YouTube para ayudarle a que recupere rápidamente el control de su cuenta.

¿Puede Bitdefender ayudarme a evitar que pirateen mi canal de YouTube?

Sí. Para evitar que su cuenta de YouTube resulte pirateada, Bitdefender le brinda consejos y le sugiere estrategias de seguridad personalizadas más allá de lo que Google le ofrece.

¿Puede Bitdefender Security for Creators protegerme contra correos electrónicos de falsos patrocinadores?

Sí, Scam Guard marca los correos electrónicos sospechosos que contienen archivos adjuntos o enlaces maliciosos, para protegerle de las estafas que se hacen pasar por ofertas de patrocinio.

¿Basta la autenticación en dos fases para proteger mi canal de YouTube frente a los piratas informáticos?

La autenticación en dos fases (2FA) constituye una capa más de seguridad, pero no es infalible. Los piratas informáticos pueden eludir la 2FA aplicando métodos como el phishing o el intercambio de SIM.

¿Puedo cambiar la cuenta de YouTube vinculada a Bitdefender Security for Creators?

Sí, puede cambiar el canal de YouTube que monitoriza en cualquier momento:

1. Inicie sesión en su cuenta de Bitdefender Central.
2. Haga clic en su nombre de usuario o en el icono de su perfil en la esquina superior derecha y seleccione **Ajustes**.
3. Haga clic en **Eliminar cuenta**.
4. Haga clic en **Conectar su cuenta** para añadir un canal de YouTube distinto.

¿Cómo puedo restaurar vídeos que se hayan eliminado de YouTube si carezco de una copia de seguridad?

Eliminar un vídeo de YouTube es una acción permanente que no puede revertirse. Una vez que los vídeos de YouTube desaparecen de su cuenta, recuperarlos puede ser todo un desafío si carece de copias de seguridad en algún almacenamiento externo o servicio en la nube. Puede intentar contactar con el servicio de soporte técnico de YouTube para solicitar ayuda,pero eso no garantiza la recuperación de los vídeos.

¿Qué hago si tengo problemas para vincular mi cuenta de YouTube?

Si tiene problemas para vincular YouTube con Bitdefender Security for Creators, lo mejor es que haga lo siguiente:

- Compruebe que su conexión a Internet es estable.
- Cerciórese de que está seleccionando la cuenta adecuada de Google correspondiente a su canal de YouTube.
- Escriba la contraseña correcta.
- Compruebe que haya otorgado todos los permisos necesarios.

2. E-MAIL PROTECTION

Su correo electrónico es una parte importante de su vida digital y, dadas sus múltiples aplicaciones en la vida real, se ha convertido en el vector de ataque preferido de los delincuentes y en una de las principales preocupaciones de ciberseguridad del usuario cotidiano.

E-mail Protection es una característica de seguridad que le permite escanear e identificar contenido potencialmente peligroso en los correos electrónicos recibidos en su bandeja de entrada. Esta característica es un paquete de una variedad de tecnologías reunidas bajo el mismo módulo de protección, como software antiphishing, antimalware, antispam, antifraude y antiestafa.

Al crear una conexión directa entre Bitdefender y su proveedor de servicios de correo electrónico, permite que el antivirus escanee sus correos electrónicos directamente y elimine las limitaciones derivadas del uso de diferentes dispositivos o clientes de correo electrónico.

Nota
Puedes proteger hasta 5 cuentas de correo electrónico diferentes.

2.1. Configurando tu cuenta

Esta característica está perfectamente integrada en la interfaz de usuario. Para comenzar a utilizar E-mail Protection:

1. Bajo **Proteccion**, haga clic **Abierto** en el **E-mail Protection** tarjeta.
2. Elija su proveedor de correo electrónico para la cuenta de correo electrónico que desea proteger.

   Nota
   E-mail Protection está actualmente disponible para cuentas de Google, cuentas de Outlook y próximamente también estará disponible para Yahoo Mail.

3. Clickea en el **Iniciar sesión** botón.
   La operación continuará entonces en su navegador.
4. Introduce tu dirección de correo electrónico y haz clic en **Próximo** botón

5. Para continuar, ingresa tu contraseña y haz clic en el **Próximo** botón.
6. Verifique los permisos solicitados en pantalla y permita que Bitdefender proteja su cuenta de correo electrónico.

Su cuenta de correo electrónico ahora está protegida y todos sus correos electrónicos entrantes nuevos serán analizados en busca de amenazas.

> **Nota**
> Cada correo electrónico escaneado estará marcado con una etiqueta para indicar sus niveles de seguridad.

2.2. Panel

El panel mostrará sus correos electrónicos protegidos, donde encontrará:

- fecha de configuración (la fecha en la que se configuró la cuenta para E-mail Protection)
- estado (activo o inactivo)
- Número de correos electrónicos filtrados en los últimos 30 días.
  Aquí verá un gráfico que muestra la cantidad de correos electrónicos seguros y peligrosos recibidos.

Para agregar varias cuentas de correo electrónico clickea en el **Agregar otra cuenta** y siga el proceso de configuración anterior para cada uno de ellos.

Para pausar el escaneo o eliminar una cuenta desde esta función, haga clic en los tres puntos al lado de la cuenta en cuestión y haga clic en **Administrar cuenta**.

3. SEGURIDAD TOTAL PARA PC

3.1. Pasos de la Instalación

3.1.1. Preparándose para la instalación

Antes de instalar Bitdefender Total Security, complete estos preparativos para garantizar la instalación sin problemas:

- Asegúrese de que el dispositivo donde piensa instalar Bitdefender cumple los requisitos del sistema. Si el dispositivo no cumple con todos los requisitos del sistema, Bitdefender no se instalará o, si estuviera instalado, no funcionaría correctamente y provocaría demoras e inestabilidad en el sistema. Para ver una lista completa de los requisitos del sistema, consulte Requisitos del sistema (página 16).
- Inicie sesión en el dispositivo utilizando una cuenta de Administrador.
- Desinstale cualquier otro software similar del dispositivo. Si se detectase alguno durante el proceso de instalación de Bitdefender, se le notificará para que lo desinstale. 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 dispositivo. 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 dispositivo esté conectado a Internet, incluso si la realiza desde un CD o DVD. Si hay disponibles versiones más recientes de los archivos de la aplicación incluidos en el paquete de instalación, Bitdefender puede descargarlas e instalarlas.

3.1.2. Requisitos del sistema

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

- Windows 7 con Service Pack 1
- Windows 8.1
- Windows 10
- 2,5 GB de espacio disponible en disco duro (al menos 800 MB en la unidad de sistema)
- 2 GB de memoria (RAM)

Importante
El rendimiento del sistema puede verse afectado en dispositivos que tengan CPU de generaciones anteriores.

Nota
Para saber qué sistema operativo Windows está ejecutando su dispositivo 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) y, luego, haga clic con el botón derecho sobre su icono. En **Windows 8.1**, busque **Este PC**. 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.

3.1.3. Requisitos de software

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

- Microsoft Edge 40 y superior
- Internet Explorer 10 y superior
- Mozilla Firefox 51 y superior
- Google Chrome 34 y superior
- Microsoft Outlook 2007 / 2010 / 2013 / 2016
- Mozilla Thunderbird 14 y superior

3.1.4. Instalando su producto Bitdefender

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

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

Instalación desde Bitdefender Central

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

Para descargar Bitdefender Total Security desde Bitdefender Central:

1. Acceda a **Bitdefender Central**.
2. Seleccione el panel **Mis dispositivos** y, a continuación, toque **INSTALAR PROTECCIÓN**.
3. Escoja una de las dos opciones disponibles:
   - **Proteger este dispositivo**
     a. Seleccione esta opción y, a continuación, seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
     b. Guarde el archivo de instalación.
   - **Proteger otros dispositivos**
     a. Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
     b. Toque **ENVIAR ENLACE DE DESCARGA**.
     c. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR CORREO ELECTRÓNICO**.
     Tenga en cuenta que el enlace de descarga generado solo es válido durante las próximas 24 horas. Si caducase, debería generar uno nuevo siguiendo los mismos pasos.

d. En el dispositivo en que desee instalar su producto Bitdefender, compruebe la cuenta de correo electrónico que introdujo y luego haga clic en el botón de descarga correspondiente.

4. Espere a que finalice la descarga y, acto seguido, ejecute el instalador.

Validación de la instalación

Bitdefender comprueba primero su sistema para validar la instalación.

Si su sistema no cumple con los requisitos del sistema para la instalación de Bitdefender, se le informará de las áreas que precisan alguna mejora para poder continuar.

Si se detecta una solución de seguridad incompatible o una versión anterior de Bitdefender, se le solicitará que la 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 dispositivo para completar la eliminación de las soluciones de seguridad detectadas.

El paquete de instalación de Bitdefender Total Security se actualiza constantemente.

> **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, aparece el asistente de configuración. Siga los pasos para instalar Bitdefender Total Security.

Paso 1 - Instalación de Bitdefender

Antes de proceder a la instalación, debe aceptar el Acuerdo de suscripción. Dedique un momento a leerlo, dado que contiene los términos y condiciones bajo los cuales puede usar Bitdefender Total Security.

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

Pueden realizarse dos tareas adicionales en este paso:

- Mantenga habilitada la opción **Enviar informes del producto**. 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.

Haga clic en el botón **INSTALAR** para iniciar el proceso de instalación de su producto Bitdefender.

Paso 2 - Instalación en curso

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

Paso 3 - 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 amenaza activa, puede que necesite reiniciar su equipo.

Paso 4 - Análisis del dispositivo

Ahora se le preguntará si desea realizar un análisis de su dispositivo para asegurarse de que sea seguro. Durante este paso, Bitdefender analizará las áreas críticas del sistema. Haga clic en **Iniciar análisis del dispositivo** para ponerlo en marcha.

Puede ocultar la interfaz de análisis haciendo clic en **Ejecutar análisis en segundo plano**. Después de eso, elija si desea recibir información cuando finalice el análisis.

Cuando haya finalizado el análisis, haga clic en **Abrir interfaz de Bitdefender**.

> **Nota**
> Como alternativa, si no desea realizar el análisis, simplemente haga clic en **Omitir**.

Paso 5 - Primeros pasos

En la ventana de **Primeros pasos** 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 {1}**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 comprueba primero su sistema para validar la instalación.

Si su sistema no cumple con los requisitos del sistema para la instalación de Bitdefender, se le informará de las áreas que precisan alguna mejora para poder continuar.

Si se detecta una solución de seguridad incompatible o una versión anterior de Bitdefender, se le solicitará que la 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 dispositivo para completar la eliminación de las soluciones de seguridad detectadas.

El paquete de instalación de Bitdefender Total Security se actualiza constantemente.

> **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, aparece el asistente de configuración. Siga los pasos para instalar Bitdefender Total Security.

Paso 1 - Instalación de Bitdefender

Antes de continuar con la instalación, debe aceptar el Acuerdo de suscripción. Tómese un tiempo para leer el Acuerdo de suscripción, ya que contiene los términos y condiciones bajo los cuales puede usar Bitdefender Total Security.

Si no está de acuerdo con estos términos, cierre la ventana. Se abandonará el proceso de instalación y saldrá de la configuración.

En este paso se pueden realizar dos tareas adicionales:

- Mantener el **Enviar informes de productos** opción habilitada. Al habilitar esta opción, los informes que contienen información sobre cómo usa el producto se envían a los servidores de Bitdefender. Esta información es esencial para mejorar el producto y puede ayudarnos a brindar una mejor experiencia 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 instalar el producto.

Hacer clic **INSTALAR** para iniciar el proceso de instalación de su producto Bitdefender.

Paso 2 - Instalación en proceso

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

Paso 3 - Instalación completada

Se muestra un resumen de la instalación. Si se detectó y eliminó alguna amenaza activa durante la instalación, es posible que sea necesario reiniciar el sistema.

Paso 4: análisis del dispositivo

Ahora se le preguntará si desea realizar un análisis de su dispositivo, para asegurarse de que es seguro. Durante este paso, Bitdefender escaneará áreas críticas del sistema. Hacer clic **Iniciar análisis de dispositivos** para iniciarlo.

Puede ocultar la interfaz de escaneo haciendo clic en **Ejecutar escaneo en segundo plano**. Después de eso, elija si desea que se le informe cuando finalice el escaneo o no.

Cuando haya finalizado el análisis, haga clic en **Pasar a Crear cuenta**.

> **Nota**
> Alternativamente, si no desea realizar el escaneo, simplemente puede hacer clic en **Saltar**.

Paso 5 - Cuenta de Bitdefender

Tras completar la configuración inicial, aparece la ventana Bitdefender Account. Es necesaria una cuenta Bitdefender para poder activar el producto y utilizar sus características online. Para más información, diríjase a Bitdefender Central.

Proceder de acuerdo a su situación.

- **Quiero crear una cuenta de Bitdefender**

  1. Introduzca la información requerida en los campos correspondientes. Los datos que introduzca aquí serán confidenciales. La contraseña debe tener al menos ocho caracteres, incluir por lo menos un número o símbolo y contener mayúsculas y minúsculas.
  2. Antes de seguir adelante, debe aceptar los Términos de uso. Acceda a los Términos de uso y léalos detenidamente, ya que contienen los términos y condiciones bajo los cuales puede usar Bitdefender.
     Además, puede acceder a la Política de privacidad y leerla.
  3. Haga clic en **CREAR CUENTA**.

  > **Nota**
  > Una vez creada la cuenta, puede usar la dirección de correo electrónico y la contraseña proporcionadas para iniciar sesión en su cuenta en https://central.bitdefender.com o en la app Bitdefender Central siempre que esté instalada en uno de sus dispositivos Android o iOS. Para instalar la app Bitdefender Central en Android, debe acceder a Google Play, buscar Bitdefender Central y luego tocar la opción de instalación correspondiente. Para instalar la app Bitdefender Central en iOS, debe acceder a la AppStore, buscar Bitdefender Central y luego tocar la opción de instalación correspondiente.

- **Ya dispongo de una cuenta de Bitdefender**

1. Haga clic en **Iniciar sesión**.
2. Escriba la dirección de correo electrónico en el campo correspondiente y, a continuación, haga clic en **SIGUIENTE**.
3. Escriba su contraseña y, a continuación, haga clic en **INICIAR SESIÓN**.
   Si olvidó la contraseña de su cuenta o, sencillamente, desea cambiar la que ya estableció:
   a. Haga clic en **¿Olvidó la contraseña?**.
   b. Escriba su dirección de correo electrónico y, a continuación, haga clic en **SIGUIENTE**.
   c. Revise su bandeja de correo electrónico, escriba el código de seguridad que ha recibido y, a continuación, haga clic en **SIGUIENTE**.
   Como alternativa, puede hacer clic en **Cambiar contraseña** en el correo electrónico que le hemos enviado.
   d. Escriba la nueva contraseña que desea establecer y, luego, vuelva a escribirla. Haga clic en **GUARDAR**.

   Nota
   Si ya tiene una cuenta de MyBitdefender, puede utilizarla para acceder a su cuenta de 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 su cuenta de 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. **Quiero evaluar Bitdefender**
     En este caso, puede utilizar el producto durante un período de treinta días. Para iniciar el período de evaluación seleccione **No tengo ninguna suscripción; quiero probar el producto gratuitamente** y, a continuación, haga clic en **CONTINUAR**.

Paso 7 - Primeros pasos

En la ventana de **Primeros pasos** puede ver la información relativa a su suscripción activa.

Hacer clic **FINALIZAR** para acceder a la Bitdefender Total Security interfaz.

3.2. Gestión de su seguridad

3.2.1. Protección Antivirus

Bitdefender protege su dispositivo contra todo tipo de amenazas (malware, troyanos, spyware, rootkits, etc.). La protección que ofrece BitDefender está dividida en dos:

- **Análisis on-access** - impide que las nuevas amenazas 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 amenazas, siendo un componente esencial de cualquier programa de seguridad informática.

  > **Importante**
  > Para evitar que las amenazas infecten su dispositivo, mantenga activado **Análisis on-access**.

- **Análisis bajo demanda** - permite detectar y eliminar la amenaza 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 dispositivo para así asegurarse de que se puede acceder al mismo de forma segura. Para más información, diríjase a Análisis automático de los medios extraíbles (página 41).

Los usuarios avanzados pueden configurar excepciones de análisis si no desean que se analicen ciertos archivos o tipos de archivo. Para más información, diríjase a Configurar excepciones de análisis (página 43).

Cuando detecte una amenaza, Bitdefender intentará eliminar automáticamente el código malicioso 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, diríjase a Administración de los archivos en cuarentena (página 45).

Si su dispositivo se ha visto infectado con amenazas, consulte Eliminación de amenazas de su sistema (página 151). Para ayudarle a limpiar su

dispositivo de amenazas que no pueden eliminarse desde el propio sistema operativo Windows, Bitdefender le ofrece Entorno de rescate (página 152). Este es un entorno de confianza, especialmente diseñado para la eliminación de amenazas, lo que le permite arrancar el dispositivo independientemente de Windows. Cuando el dispositivo se ejecuta en Entorno de rescate, las amenazas de Windows están inactivas, por lo que es fácil eliminarlas.

Análisis on-access (protección en tiempo real)

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

Activar o desactivar la protección en tiempo real

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

1. Haga clic en **Protección** en el menú de navegación de la **interfaz de Bitdefender**.
2. En el panel **ANTIVIRUS**, haga clic en **Abrir**.
3. En la ventana **Avanzado**, active o desactive **Bitdefender Residente**.
4. 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.

Advertencia

Esto supone un grave problema de seguridad. Le recomendamos que desactive la protección en tiempo real lo menos posible. Si desactiva la protección en tiempo real, no estará protegido contra las amenazas.

Configuración de los ajustes avanzados de la 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 avanzados de la protección en tiempo real:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. En la ventana **Avanzado** puede personalizar los ajustes de análisis según sea necesario.

Información sobre las opciones de análisis

Puede que esta información le sea útil:

- **Analizar únicamente aplicaciones.** Puede configurar Bitdefender para que analice solo las aplicaciones a las que se accede.
- **Analizar en busca de aplicaciones potencialmente no deseadas.** Seleccione esta opción para buscar aplicaciones no deseadas. Una aplicación potencialmente no deseada (APND) o programa potencialmente no deseado (PPND) es un software que viene incluido generalmente con el freeware y mostrará ventanas emergentes o una barra de herramientas en el navegador por defecto. Algunos cambiarán la página de inicio o el motor de búsqueda, mientras que otros ejecutarán varios procesos en segundo plano, ralentizando el PC, o mostrarán numerosos anuncios. Estos programas pueden instalarse sin su consentimiento (también llamados adware) o incluirse por defecto en el kit de instalación (que tiene publicidad).
- **Analizar scripts.** La característica Analizar scripts permite que Bitdefender analice scripts de PowerShell y documentos de Office que puedan contener malware basado en scripts.
- **Analizar recursos compartidos.** Para acceder de forma segura a una red remota desde su dispositivo, le recomendamos que mantenga habilitada la opción Analizar recursos compartidos.
- **Analizar memoria de procesos.** Busca actividades maliciosas en la memoria de los procesos en ejecución.
- **Analizar línea de comandos.** Analiza la línea de comandos de las aplicaciones iniciadas recientemente para evitar ataques sin archivos.

- **Analizar archivos comprimidos.** Analizar el contenido de los archivos comprimidos es un proceso lento que consume muchos recursos, por lo que no se recomienda para la protección en tiempo real. Los archivos comprimidos que contienen archivos infectados no representan una amenaza inmediata para la seguridad del sistema. Las amenazas pueden afectar a su sistema solo si el archivo infectado es extraído del archivo comprimido y ejecutado sin tener la protección en tiempo real activada.

  Si decide utilizar esta opción, actívela y, a continuación, arrastre el control deslizante por la escala para excluir del análisis los archivos que superen determinado tamaño indicado en MB (Megabytes).

- **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 informático necesario para iniciar el proceso de arranque. Cuando una amenaza infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar su sistema y acceder a sus datos.

- **Analizar solo los archivos nuevos o modificados.** Al analizar únicamente los archivos nuevos o modificados, puede mejorar en gran medida la capacidad de respuesta general del sistema comprometiendo mínimamente la 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 pirata informático puede hallar información confidencial en los datos robados, como números de cuentas bancarias y contraseñas, y utilizarla en su propio beneficio.

- **Análisis de arranque.** 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 amenazas en el inicio del sistema, así como el tiempo de arranque del mismo.

Medidas adoptadas sobre las amenazas detectadas

Puede configurar las acciones llevadas a cabo por la protección en tiempo real siguiendo los pasos que se indican a continuación:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. En la ventana **Avanzado**, desplácese hacia abajo hasta que aparezca la opción **Acciones de amenazas**.
4. Configure los ajustes del análisis como necesite.

La protección en tiempo real de Bitdefender puede llevar a cabo las siguientes acciones:

Tomar las medidas adecuadas

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

- **Archivos infectados.** Los archivos detectados como infectados coinciden con la información sobre amenazas encontrada en la base de datos de Bitdefender. Bitdefender intentará automáticamente eliminar el código malicioso 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, diríjase a {1}{2}.

  Importante
  En ciertos tipos de amenazas, la desinfección no es posible porque el archivo detectado es completamente malicioso. En estos casos, el archivo infectado es borrado del disco.

- **Archivos sospechosos.** El análisis heurístico detecta los archivos sospechosos. Los archivos sospechosos no pueden desinfectarse porque no existe una rutina de desinfección disponible. Estos se trasladarán a la cuarentena para evitar una posible infección.
- **Archivos comprimidos 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.

Pasar a la 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, diríjase a Administración de los archivos en cuarentena (página 45).

Denegar el acceso

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

Restaurar la configuración predeterminada

Los ajustes por defecto de protección en tiempo real garantizan una buena defensa contra las amenazas con escaso impacto en el rendimiento del sistema.

Para restaurar la configuración predeterminada de la protección en tiempo real:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. En la ventana **Avanzado**, desplácese hacia abajo hasta que aparezca la opción {3}Reiniciar ajustes avanzados{4}. Seleccione esta opción para reiniciar los ajustes del antivirus y que adopten los valores por defecto.

Análisis solicitado

El objetivo principal de Bitdefender es mantener su dispositivo limpio de amenazas. Esto se consigue manteniendo las nuevas amenazas fuera de su dispositivo y analizando los mensajes de correo y cualquier archivo nuevo descargado o copiado a su sistema.

Existe el riesgo de que ya exista una amenaza en su sistema, antes siquiera de instalar Bitdefender. Por eso es buena idea analizar su dispositivo en busca de amenazas preexistentes nada más instalar

Bitdefender. Y, desde luego, es buena idea analizar frecuentemente su dispositivo en busca de amenazas.

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 dispositivo 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 dispositivo o configurar las opciones de análisis, configure y ejecute un análisis personalizado.

Analizar un archivo o una carpeta en busca de amenazas

Debe analizar los archivos y carpetas cuando 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**. Aparecerá el **Asistente de análisis antivirus** que le guiará durante este proceso. Al final del análisis, se le pedirá que elija las acciones que desea llevar a cabo sobre los archivos detectados, si se encontrase alguno.

Ejecución de un análisis Quick Scan

QuickScan utiliza el análisis en la nube para detectar amenazas que se estén ejecutando en su sistema. La ejecución de QuickScan tarda por lo general menos de un minuto y utiliza una fracción de los recursos del sistema necesarios para un análisis antivirus normal.

Para ejecutar un análisis Quick Scan:

1. Haga clic en Protección en el menú de navegación de la interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. En la ventana de **Análisis**, haga clic en el botón **Ejecutar análisis** junto a **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.

Ejecución de un análisis del sistema

La tarea de análisis del sistema analiza todo el dispositivo en busca de todo tipo de amenazas que pongan en peligro su seguridad, como malware, 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 dispositivo.

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

- Asegúrese de que Bitdefender está actualizado con su base de datos de información de amenazas. Analizar su dispositivo con una base de datos de información de amenazas obsoleta puede impedir que Bitdefender detecte nuevas amenazas encontradas desde la última actualización. Para más información, diríjase a Mantener Bitdefender al día.
- Cierre todos los programas abiertos.

Si desea analizar ubicaciones específicas en el dispositivo o configurar las opciones de análisis, configure y ejecute un análisis personalizado. Para más información, diríjase a Configuración de un análisis personalizado (página 34).

Para ejecutar un Análisis del sistema:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. En la ventana **Análisis**, haga clic en el botón **Ejecutar análisis** junto a **Análisis del sistema**.
4. La primera vez que ejecuta un Análisis del sistema, se le presenta esta característica. Haga clic en **Bien, entendido** para continuar.
5. Siga el Asistente de análisis antivirus para completar el escaneo. Bitdefender realizará automáticamente las acciones recomendadas en los archivos detectados. Si quedan amenazas sin resolver, se le pedirá que elija las acciones que se van a realizar sobre ellas.

Configuración de un análisis personalizado

En la ventana **Administrar análisis**, puede configurar Bitdefender para que ejecute análisis siempre que considere que su dispositivo necesita comprobar la presencia de posibles amenazas. Puede elegir programar un **Análisis del sistema** o un **Quick Scan**, o también puede crear un análisis personalizado si lo prefiere.

Para configurar detalladamente un nuevo análisis personalizado:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. En la ventana **Análisis**, haga clic en **+Crear análisis**.
4. En el campo **Nombre de la tarea**, escriba un nombre para el análisis, luego seleccione las ubicaciones que le gustaría analizar y, a continuación, haga clic en **Siguiente**.
5. Configure estas opciones generales:
   - **Escanear solo aplicaciones.** Puede configurar Bitdefender para analizar solo las aplicaciones a las que se accede.
   - **Prioridad de la tarea de análisis.** Puede elegir el impacto que el proceso de análisis debería tener en el rendimiento de su sistema.
     - Automático: La prioridad del proceso de análisis dependerá de la actividad del sistema. Para asegurarse de que el proceso de análisis no afecte a la actividad del sistema, Bitdefender decidirá si este debe ejecutarse con prioridad alta o baja.
     - Alta: La prioridad del proceso de análisis será alta. Al escoger esta opción, permitirá que otros programas se ejecuten más despacio y reducirá el tiempo necesario para que finalice el análisis.
     - Baja: La prioridad del proceso de análisis será baja. Al escoger esta opción, permitirá que otros programas se ejecuten más rápidamente y aumentará el tiempo necesario para que finalice el análisis.
   - **Acciones posteriores al análisis.** Elija la acción que debe llevar a cabo Bitdefender en caso de que no se encuentren amenazas:

- Mostrar ventana resumen
- Apagar el dispositivo
- Cerrar ventana de análisis

6. Si desea configurar detalladamente las opciones de análisis, haga clic en **Mostrar opciones avanzadas**. Puede encontrar información sobre la lista de análisis al final de esta sección.
   Haga clic en **Siguiente**.
7. Si lo desea, puede habilitar **Programar tarea de análisis** y, a continuación, elegir cuándo debe iniciarse el análisis personalizado que ha creado.
   - Al iniciar el sistema
   - Diariamente
   - Mensualmente
   - Semanalmente

   Si elige Diariamente, Semanalmente o Mensualmente, arrastre el control deslizante sobre la escala para establecer el período de tiempo deseado en que debe iniciarse el análisis programado.
8. Haga clic en **Guardar** para guardar los ajustes y cierre la ventana de configuración.
   Dependiendo de las ubicaciones a analizar, el análisis puede llevar más tiempo. Si se encuentran amenazas durante el proceso de análisis, se le pedirá que elija las acciones que desea llevar a cabo sobre los archivos detectados.

Información sobre las opciones de escaneo

Usted puede encontrar esta información útil:

- Si no se familiariza con algunos términos, compruebe estos en el **glosario**. También puede encontrar información de utilidad buscando en internet.
- **Escanee aplicaciones potencialmente no deseadas.** Seleccione esta opción para buscar aplicaciones no deseadas. Una aplicación potencialmente no deseada (PUA, por sus siglas en inglés) o un programa potencialmente no deseado (PUP, por sus siglas en inglés) es un software que generalmente viene incluido con un software

gratuito y mostrará ventanas emergentes o instalará una barra de herramientas en el navegador predeterminado. Algunos de ellos cambiarán la página de inicio o el motor de búsqueda, otros ejecutarán varios procesos en segundo plano ralentizando la PC o mostrarán numerosos anuncios. Estos programas se pueden instalar sin su consentimiento (también denominados adware) o se incluirán de manera predeterminada en el kit de instalación rápida (con publicidad).

- **Análisis de archivos comprimidos.** Los archivos comprimidos que contienen archivos infectados no representan una amenaza inmediata para la seguridad del sistema. Las amenazas pueden afectar a su sistema solo si el archivo infectado es extraído del archivo comprimido y ejecutado sin tener la protección en tiempo real activada. No obstante, se recomienda usar esta opción con el fin de detectar y eliminar cualquier amenaza potencial, incluso aunque no se trate de una amenaza inmediata.
  Arrastre el control deslizante por la escala para excluir del análisis los archivos que superen determinado tamaño indicado en MB (Megabytes).

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

- **Escanee solo archivos nuevos y modificados.** Al escanear solo archivos nuevos y modificados, puede mejorar en gran medida la capacidad de respuesta general del sistema con una compensación mínima en seguridad.
- **Escanear sectores de arranque.** Puede configurar Bitdefender para escanear los sectores de arranque de su disco duro. Este sector del disco duro contiene el código informático necesario para iniciar el proceso de arranque. Cuando una amenaza infecta el sector de arranque, la unidad puede volverse inaccesible y es posible que no pueda iniciar su sistema y acceder a sus datos.
- **Analizar la memoria.** Seleccione esta opción para analizar programas que se ejecuten en la memoria de su sistema.
- **Analizar el Registro.** Seleccione esta opción para analizar las claves del 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 las cookies.** Seleccione esta opción para analizar las cookies almacenadas por los navegadores en su dispositivo.
- **Escanear registradores de teclas.** Seleccione esta opción para escanear su sistema en busca de aplicaciones de registro de teclas. Los keyloggers registran lo que escribe en su teclado y envían informes a través de Internet a una persona malintencionada (hacker). El pirata informático puede encontrar información confidencial de los datos robados, como números de cuentas bancarias y contraseñas, y utilizarla para obtener beneficios personales.

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 Análisis de Bitdefender Antivirus. Siga el asistente para completar el proceso de análisis.

> **Nota**
> Si no aparece el asistente de análisis, este puede configurarse para que se ejecute discretamente, en segundo plano. Busque el icono de progreso del análisis en la **bandeja del sistema**. Puede hacer clic en este icono para abrir la ventana de análisis y consultar su avance.

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 poner en pausa el análisis. Puede detener el análisis en cualquier momento haciendo clic en **DETENER**. Pasará directamente al último paso del asistente. Para detener temporalmente el proceso de análisis, haga clic en **PAUSA**. Tendrá que hacer clic en **REANUDAR** para retomar el análisis.

Archivos comprimidos protegidos con contraseña. Si se detecta un archivo protegido por contraseña puede que, dependiendo de los ajustes

del análisis, se le solicite que proporcione la contraseña. Los archivos comprimidos protegidos con contraseña no se pueden analizar a menos que proporcione su contraseña. Tiene a su disposición las siguientes opciones:

- **Contraseña.** Si desea que Bitdefender analice el archivo comprimido, seleccione esta opción e introduzca la contraseña. Si desconoce la contraseña, elija una de las otras opciones.
- **No pedir contraseña y omitir este objeto del análisis.** Seleccione esta opción para omitir el análisis de este archivo comprimido.
- **Omitir todos los elementos protegidos con contraseña sin analizarlos.** Seleccione esta opción si no quiere que se le moleste por los archivos protegidos con contraseña. Bitdefender no podrá analizarlos, pero se realizará una anotación en el registro 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 en grupos, según las amenazas con las que estén infectados. 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:

Tomar las medidas adecuadas

Bitdefender tomará las acciones recomendadas según el tipo de archivo detectado:

- **Archivos infectados.** Los archivos detectados como infectados coinciden con la información sobre amenazas que se encuentra en

la base de datos de información sobre amenazas de Bitdefender. Bitdefender intentará eliminar automáticamente el código malicioso del archivo infectado y reconstruir el archivo original. Esta operación se denomina desinfección.

Los archivos que no se pueden desinfectar se mueven a la cuarentena para contener la infección. Los archivos en cuarentena no se pueden ejecutar ni abrir; por lo tanto, el riesgo de infectarse desaparece. Para obtener más información, consulte Administración de los archivos en cuarentena (página 45).

> **Importante**
> Para determinados tipos de amenazas, la desinfección no es posible porque el archivo detectado es completamente malicioso. En tales casos, el archivo infectado se elimina del disco.

- **Archivos sospechosos.** El análisis heurístico detecta los archivos como sospechosos. Los archivos sospechosos no se pueden desinfectar porque no hay una rutina de desinfección disponible. Serán trasladados a cuarentena para prevenir una posible infección.
- **Archivos que contienen archivos infectados.**
  - Los archivos que contienen solo archivos infectados se eliminan automáticamente.
  - Si un archivo contiene archivos infectados y limpios, Bitdefender intentará eliminar los archivos infectados siempre que pueda reconstruir el archivo con los archivos limpios. Si la reconstrucción del archivo no es posible, se le informará que no se puede tomar ninguna medida para evitar la pérdida de 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.

No realizar 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 completa sobre el proceso de análisis, haga clic en **MOSTRAR REGISTRO** para ver el registro de análisis.

> **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, reinicie su equipo para completar el proceso de desinfección. Para obtener más información e instrucciones sobre cómo eliminar manualmente una amenaza, consulte Eliminación de amenazas de su sistema (página 151).

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 finalizado este, haciendo clic en **MOSTRAR REGISTRO**.

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

1. Hacer clic **Notificaciones** en el menú de navegación 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 amenazas, incluyendo las 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 cuando está activada la opción de Autoanálisis. Esto se recomienda con el fin de evitar que su dispositivo se infecte con amenazas.

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

- Cds/DVDs
- Unidades flash, 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 busca de amenazas (siempre y cuando se haya habilitado el análisis automático para este tipo). Mediante una ventana emergente se le notificará que se ha detectado un nuevo dispositivo y se está analizando.

Aparecerá un icono de análisis de Bitdefender en la **bandeja del sistema**. Puede hacer clic en este icono para abrir la ventana de análisis y consultar su avance.

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.

En la mayoría de los casos, Bitdefender elimina automáticamente las amenazas detectadas o mantiene aislados en cuarentena los archivos

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

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

Esta información le puede ser útil:

- Tenga cuidado al usar un CD/DVD infectado con una amenaza, porque esta no puede eliminarse del disco (el soporte es de solo lectura). Asegúrese de que la protección en tiempo real está activada para evitar que las amenazas se propaguen 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 amenazas de determinados archivos 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 averiguar cómo enfrentarse a las amenazas, consulte Eliminación de amenazas de su sistema (página 151).

Administrar el análisis de medios extraíbles

Para gestionar el análisis automático de medios extraíbles:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. Seleccione la ventana **Ajustes**.

Las opciones de análisis están preconfiguradas para mejores resultados de detección. Si se detectan archivos infectados, Bitdefender intentará desinfectarlos (eliminando el código malicioso). 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.

Para una mejor protección, se recomienda dejar seleccionada la opción de **Autoanálisis** para todos los tipos de dispositivos de almacenamiento extraíbles.

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. Hacer clic **Ajustes** en el menú de navegación de la Interfaz de Bitdefender.
2. Selecciona el **Avanzado** pestaña.
3. Active o desactive el **análisis del archivo hosts**.

Configurar excepciones de análisis

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

Puede configurar excepciones para aplicar solamente al análisis en tiempo real o bajo demanda, o a ambos. No se analizarán los objetos exceptuados del análisis on-access, ya sean accedidos por usted o por una app.

> **Nota**
> NO se aplicarán las excepciones al análisis contextual. 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**.

Exceptuar del análisis los archivos o carpetas

Para exceptuar determinados archivos y carpetas del análisis:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. En la ventana **Ajustes**, haga clic en **Administrar excepciones**.
4. Haga clic en **+Añadir una excepción**.
5. Introduzca en el campo correspondiente la ruta de la carpeta que desea exceptuar del análisis.
   Como alternativa, puede navegar hasta la carpeta haciendo clic en el botón Examinar de la derecha de la interfaz, seleccionarla y hacer clic en **Aceptar**.
6. Active el conmutador junto a la característica de protección que no debe analizar la carpeta. Hay tres opciones:
   - Antivirus
   - Prevención de amenazas online
   - Advanced Threat Defense
7. Haga clic en **Guardar** para guardar los cambios y cerrar la ventana.

Exceptuar del análisis las extensiones de archivo

Al exceptuar una extensión de archivo del análisis, Bitdefender ya no analizará archivos con esa extensión, independientemente de la ubicación en su dispositivo. La excepción también se aplica a los archivos en medios extraíbles, como CD, DVD, dispositivos de almacenamiento USB o unidades de red.

> **Importante**
> Tenga cuidado al exceptuar las extensiones del análisis ya que tales excepciones pueden hacer que su dispositivo sea vulnerable a las amenazas.

Para exceptuar extensiones de archivo del análisis:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.

2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. En el **Ajustes** ventana, haga clic **Administrar excepciones**.
4. Hacer clic **+Agregar una excepción**.
5. Escriba las extensiones que desea exceptuar del análisis con un punto delante, separándolas con punto y coma (;).
   txt;avi;jpg
6. Active el conmutador junto a la característica de protección que no debe analizar la extensión.
7. Haga clic en **Guardar**.

Administrar excepciones de análisis

Si las excepciones de análisis configuradas dejan de ser necesarias, se recomienda que las elimine o desactive las excepciones de análisis.

Para administrar las excepciones del análisis:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. En la ventana **Ajustes**, haga clic en **Administrar excepciones**. Se mostrará una lista con todas sus excepciones.
4. Para eliminar o editar excepciones del análisis, haga clic en uno de los botones disponibles. Siga estos pasos:
   - Para eliminar un elemento de la lista, haga clic en el botón junto a él.
   - Para editar un elemento de la tabla, haga clic en el botón **Editar** junto a él. Aparece una nueva ventana donde podrá cambiar la extensión o la ruta que desee exceptuar, así como la característica de seguridad de la que desea exceptuarla. Realice los cambios necesarios y haga clic en **MODIFICAR**.

Administración de los archivos en cuarentena

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

Además, Bitdefender analiza los archivos en cuarentena cada vez que se actualiza la base de datos de información de amenazas. Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.

Para comprobar y administrar los archivos en cuarentena:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. Acceda a la ventana **Ajustes**.
   Aquí puede ver el nombre de los archivos en cuarentena, su ubicación original y el nombre de las amenazas detectadas.
4. Bitdefender gestiona automáticamente los archivos en cuarentena, según la configuración de cuarentena predeterminada.
   Aunque no es recomendable, puede ajustar la configuración de la cuarentena según sus preferencias haciendo clic en **Ver ajustes**.
   Haga clic en los conmutadores para activar o desactivar:
   Volver a analizar la cuarentena tras actualizar la información de amenazas
   Mantenga activada esta opción para analizar automáticamente los archivos en cuarentena después de cada actualización de la base de datos de información de amenazas. Los ficheros desinfectados serán trasladados automáticamente a su ubicación original.
   Eliminar contenido con una antigüedad superior a 30 días
   Los archivos con antigüedad superior a 30 días se eliminan automáticamente.
   Crear excepciones para los archivos restaurados
   Los archivos que restaura desde la cuarentena vuelven a su ubicación original sin ser reparados y se exceptúan automáticamente de futuros análisis.
5. Para eliminar un archivo en cuarentena, selecciónelo y haga clic en el botón **Eliminar**. Si desea restaurar una archivo en cuarentena a su ubicación original, selecciónelo y haga clic en **Restaurar**.

3.2.2. Defensa contra amenazas avanzadas

Advanced Threat Defense 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.

Advanced Threat Defense monitoriza continuamente las aplicaciones que se están ejecutando en su dispositivo, buscando acciones propias de amenazas. Cada una de estas acciones se puntúa y se calcula una puntuación global para cada proceso.

Como medida de seguridad, se le notificará cada vez que se detecten y bloqueen procesos potencialmente maliciosos.

Activar o desactivar Defensa Contra Amenazas Avanzadas

Para activar o desactivar Defensa Contra Amenazas Avanzadas:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el panel **ADVANCED THREAT DEFENSE**, haga clic en **Abrir**.
3. Acceda a la ventana **Ajustes** y haga clic en el conmutador junto a **Bitdefender Advanced Threat Defense**.

> **Nota**
> Para mantener su sistema a salvo de ransomware y de otras amenazas, le recomendamos que desactive Advanced Threat Defense durante el menor tiempo posible.

Comprobación de los ataques maliciosos detectados

Siempre que se detecten amenazas o procesos potencialmente maliciosos, Bitdefender los bloqueará para evitar que su dispositivo resulte infectado por ransomware u otro malware. Puede consultar en cualquier momento la lista de ataques maliciosos detectados siguiendo los pasos que se exponen a continuación:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **DEFENSA AVANZADA CONTRA AMENAZAS** panel, haga clic **Abierto**.
3. Acceda a la ventana **Threat Defense**.
   Se muestran los ataques detectados durante los últimos noventa días. Para obtener detalles acerca del tipo de ransomware detectado, la ruta del proceso malicioso, o si la desinfección tuvo éxito, simplemente haga clic en el elemento.

Añadir procesos a las excepciones

Puede configurar reglas de excepción para las apps de confianza, de modo que Advanced Threat Defense no las bloquee si realizan acciones típicas de amenazas.

Para empezar a añadir procesos a la lista de excepciones de Advanced Threat Defense:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **DEFENSA AVANZADA CONTRA AMENAZAS** panel, haga clic **Abierto**.
3. En el **Ajustes** ventana, haga clic **Administrar excepciones**.
4. Hacer clic **+Agregar una excepción**.
5. Introduzca la ruta de la carpeta que desea excluir del análisis en el campo correspondiente.
   Como alternativa, puede navegar hasta el ejecutable haciendo clic en el botón Examinar de la derecha de la interfaz, seleccionarlo y hacer clic en **Aceptar**.
6. Active el conmutador junto a **Advanced Threat Defense**.
7. Hacer clic **Ahorrar**.

Detección de exploits

Una de las formas empleadas por los piratas informáticos para introducirse en los sistemas es aprovechar determinados errores o vulnerabilidades de los programas informáticos (aplicaciones o complementos) y del hardware. Para asegurarse de que su dispositivo permanezca a salvo de esos ataques, que normalmente se propagan muy rápidamente, Bitdefender utiliza las tecnologías antiexploit más recientes.

Activar o desactivar la detección de exploits

Para activar o desactivar la detección de exploits:

- Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
- En el **DEFENSA AVANZADA CONTRA AMENAZAS** panel, haga clic **Abierto**.

- Acceda a la ventana **Ajustes** y haga clic en el conmutador junto a **Detección de exploits** para activar o desactivar la característica.

> **Nota**
> La opción de detección de exploits está activada por defecto.

3.2.3. Prevención de amenazas en línea

La Prevención de amenazas online de Bitdefender le garantiza una navegación segura por Internet alertándole sobre posibles páginas web maliciosas.

Bitdefender proporciona prevención de amenazas online en tiempo real para:

- Internet Explorer
- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari
- Bitdefender Safepay™
- Opera

Para configurar los ajustes de la Prevención de amenazas online:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el panel **PREVENCIÓN DE AMENAZAS ONLINE**, haga clic en **Ajustes**.

En las secciones **Protección web**, haga clic en los conmutadores para activar o desactivar:

- La prevención de ataques web bloquea las amenazas procedentes de Internet, incluyendo las descargas ocultas.
- 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 que albergue contenidos peligrosos. Tenga cuidado si desea visitarla.

Esta es una página 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 sitios web cifrados.
  Los ataques más sofisticados pueden utilizar el tráfico de Internet seguro para engañar a sus víctimas. Por lo tanto, le recomendamos que mantenga habilitada la opción de Análisis de sitios web cifrados.
- Protección contra fraude.
- Protección contra phishing.

Desplácese hacia abajo y llegará a la sección de **Prevención de amenazas de red**. Aquí tiene la opción de **Prevención de amenazas de red**. Para mantener su dispositivo a salvo de los ataques de malware complejo (como el ransomware) a través del aprovechamiento de vulnerabilidades, mantenga esta opción habilitada.

Puede crear una lista de sitios web, dominios y direcciones IP que no serán analizados por los motores antiphishing, antifraude y contra amenazas de Bitdefender. La lista debería contener únicamente sitios web, dominios y direcciones IP en los que confíe plenamente.

Para configurar y administrar sitios web, dominios y direcciones IP utilizando la característica de Prevención de amenazas online ofrecida por Bitdefender:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.

2. En el **PREVENCIÓN DE AMENAZAS EN LÍNEA** panel, haga clic **Ajustes**.
3. Haga clic en **Administrar excepciones**.
4. Hacer clic **+Agregar una excepción**.
5. Escriba en el campo correspondiente el nombre del sitio web, el nombre del dominio o la dirección IP que desea añadir a las excepciones.
6. Haga clic en el conmutador junto a **Prevención de amenazas online**.
7. Para eliminar una entrada de la lista, haga clic en el botón botón al lado.
   Hacer clic **Ahorrar** 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 qué hacer a continuación. Tiene a su disposición las siguientes opciones:

- Abandone 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**.
- Si sabe a ciencia cierta que el sitio web detectado es seguro, haga clic en **ENVIAR** para añadirlo a la lista blanca. Le recomendamos que solo añada sitios web en los que confíe plenamente.

3.2.4. 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 la Bandeja de entrada del usuario. Para más información, diríjase a Conocimientos antispam (página 52).

La protección antispam de Bitdefender está disponible únicamente para clientes de correo configurados para recibir mensajes a través del protocolo POP3. POP3 es uno de los protocolos más ampliamente utilizados para descargar mensajes de correo electrónico desde un servidor.

> **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 de spam detectados por Bitdefender llevan [spam] delante de la línea de asunto. Bitdefender traslada automáticamente los mensajes de spam a una carpeta concreta, 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 de **Spam** se crea cuando se etiqueta un correo electrónico como spam.
- En Mozilla Thunderbird los mensajes de spam se trasladan automáticamente a la carpeta **Spam**, ubicada en la carpeta **Papelera**. La carpeta de **Spam** se crea cuando un mensaje de correo electrónico se etiqueta como spam.

Si utiliza otros clientes de correo, debe crear una regla para trasladar los mensajes de correo electrónico marcados por Bitdefender como [spam] a una carpeta de cuarentena personalizada. Si se suprime la carpeta de Papelera o de Elementos eliminados, también se eliminará la carpeta de Spam. No obstante, se creará una nueva carpeta de Spam en cuanto se etiquete como tal un mensaje de correo electrónico.

Conocimientos antispam

El antispam presenta las siguientes características y ajustes:

Los Filtros Antispam

El motor antispam de Bitdefender incorpora protección en la nube y otros filtros que garantizan que su buzón quede libre de spam, como la

Lista de amigos, la **Lista de emisores de spam** y el **Filtro de juegos 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**. BitDefender no 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

Muchos mensajes de spam llegan escritos en caracteres cirílicos o asiáticos. El Filtro de juegos de caracteres detecta este tipo de mensajes y los marca como spam.

Manejo de Antispam

El motor antispam de Bitdefender utiliza todos los filtros antispam combinados para determinar si cierto mensaje de correo electrónico debe llegar o no a su **bandeja de entrada**.

Todo mensaje procedente de Internet se coteja en primer lugar con los filtros de la **lista de amigos** o la de **emisores de spam**. Si encuentra la dirección del remitente en la **Lista de amigos**, el mensaje pasa 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 mensaje se etiqueta en la línea de asunto como SEXUALMENTE EXPLÍCITO, 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 / 2016 / 2019
- Mozilla Thunderbird 14 y versiones posteriores

Activar o desactivar la protección antispam

La protección antispam está habilitada por omisión.

Para activar o desactivar la característica Antispam:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el panel **ANTISPAM**, active o desactive el conmutador.

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, diríjase a Clientes de correo electrónico y protocolos soportados (página 54).

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

Ajustes: Abre una ventana donde puede configurar los filtros antispam y las opciones de la barra de herramientas.

Es spam: Indica que el mensaje de correo electrónico seleccionado es spam. El mensaje de correo electrónico se trasladará de inmediato a la

carpeta de **Spam**. Si están activados los servicios antispam en la nube, se envía el mensaje a la Bitdefender Cloud para su posterior análisis.

No es spam: Indica que el mensaje de correo electrónico seleccionado no es spam y Bitdefender no debería haberlo etiquetado como tal. El mensaje de correo electrónico se trasladará de la carpeta **Spam** a la **Bandeja de entrada**. Si están activados los servicios antispam en la nube, se envía el mensaje a la Bitdefender Cloud para su posterior análisis.

> **Importante**
>
> El botón **No es spam** se activa cuando selecciona un mensaje marcado por Bitdefender como SPAM (normalmente, estos se encuentran en la carpeta de **Spam**).

Añadir emisor de spam: Añade el remitente del mensaje de correo electrónico seleccionado a la lista de emisores de spam. Puede que tenga que hacer clic en **Aceptar** para confirmar esta acción. Los mensajes de correo electrónico recibidos de direcciones que se encuentren en la Lista de emisores de spam se marcarán automáticamente como [spam].

Añadir amigo: Añade el remitente del mensaje de correo electrónico seleccionado a la Lista de amigos. Puede que tenga que hacer clic en **Aceptar** para confirmar esta acción. Siempre recibirá mensajes de correo electrónico de esta dirección, independientemente de su contenido.

Emisores de spam: Abre la **Lista de emisores de spam** que contiene todas las direcciones de correo electrónico desde las que no desea recibir mensajes, independientemente de su contenido. Para obtener más información, consulte Configurando la Lista de Spammers (página 58).

Amigos: Abre la **Lista de amigos** que contiene todas las direcciones de correo electrónico desde las que siempre desea recibir mensajes, independientemente de su contenido. Para obtener más información, consulte Configurando la Lista de Amigos (página 57).

Indicar los errores de detección

Si está utilizando un cliente de correo compatible, puede corregir fácilmente el filtro antispam (indicando qué mensajes no deben marcarse como [spam]). Haciendo esto aumentará considerablemente la eficacia del filtro antispam. Para ello, siga los pasos que se exponen a continuación:

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 legítimo marcado incorrectamente por Bitdefender como [**spam**].
4. Haga clic en el botón **Añadir amigo** de la barra de herramientas antispam de Bitdefender para añadir el remitente a la Lista de amigos. Puede que tenga que hacer clic en **Aceptar** para confirmar esta acción. Siempre recibirá mensajes de correo electrónico 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. Abre tu 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 (normalmente se encuentra en la parte superior de la ventana del cliente de correo). Se marcan inmediatamente como [spam] y se trasladan a la carpeta de spam.

Configurar las opciones de la barra de herramientas

Para configurar los ajustes de la barra de herramientas antispam en su cliente de correo electrónico, haga clic en el botón **Ajustes** 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 emisor de spam** y **Añadir amigo** de la barra de herramientas 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**
> Cualquier correo procedente de una dirección contenida en la **Lista de amigos** se enviará a su bandeja de entrada sin mayor proceso.

Para configurar y administrar la lista de Amigos:

- Si utiliza Microsoft Outlook o Thunderbird, haga clic en el botón Amigos de la **barra de herramientas antispam de Bitdefender**.
- Como alternativa:
  1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
  2. En el panel **ANTISPAM**, haga clic en **Ajustes**.
  3. Acceda a la ventana **Gestionar amigos**.

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

Para añadir todas las direcciones de correo electrónico de un dominio específico, seleccione la opción **Nombre de dominio**, introduzca el nombre de dominio y, a continuación, haga clic en el botón **AÑADIR**. Sintaxis:

- @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) 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. 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 botón correspondiente junto a él. Para eliminar todos los elementos de la lista, haga clic en **Borrar lista**.

Puede guardar la lista de Amigos a un archivo la cual puede utilizarse en otro dispositivo 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 guardada previamente, haga clic en **Cargar** y abra el archivo .bwl correspondiente. Para reiniciar el contenido de la lista existente al cargar una lista previamente guardada, marque la casilla junto a **Sobrescribir la lista actual**.

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 utiliza Microsoft Outlook o Thunderbird, haga clic en el botón **Emisores de spam** de la **barra de herramientas antispam de Bitdefender** integrada en su cliente de correo.
- Alternativamente:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTISPAM** panel, haga clic **Ajustes**.
3. Acceda a la ventana **Gestionar emisores de spam**.

Para agregar una dirección de correo electrónico, seleccione la **Dirección de correo electrónico** opción, ingrese la dirección y luego haga clic en **AGREGAR**. Sintaxis: nombre@dominio.com.

Para agregar todas las direcciones de correo electrónico de un dominio específico, seleccione el **Nombre de dominio** opción, ingrese el nombre de dominio y luego haga clic en **AGREGAR**. Sintaxis:

- @dominio.com y dominio.com: todos los mensajes de correo electrónico recibidos de dominio.com llegarán a su **Bandeja de entrada**, independientemente de su contenido.
- dominio: todos los mensajes de correo electrónico recibidos del dominio (sin importar los sufijos del dominio) se etiquetarán 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.

Advertencia

No añada a la lista de emisores de spam dominios de servicios legítimos de correo electrónico basados en la web (como Yahoo, Gmail, Hotmail, etc.). De lo contrario, los mensajes recibidos de cualquier usuario registrado en dichos servicios se detectarán como spam. Si, por ejemplo, añade **yahoo.com** a la lista de emisores de spam, todos los mensajes de correo electrónico procedentes de las direcciones de **yahoo.com** se marcarán como [spam].

Para eliminar un elemento de la lista, haga clic en el correspondiente botón al lado. Para eliminar todas las entradas de la lista, haga clic en **Limpiar lista**.

Puede guardar la lista de Amigos a un archivo la cual puede utilizarse en otro dispositivo 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 emisores de spam guardada previamente, haga clic en **CARGAR** y abra el archivo .bwl correspondiente. Para reiniciar el contenido de la lista existente al cargar una lista previamente guardada, seleccione Sobrescribir la lista actual.

Configuración de los filtros antispam locales

Cómo Conocimientos antispam (página 52) se describe en , 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. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTISPAM** panel, haga clic **Ajustes**.
3. Acceda a la ventana **Ajustes** y haga clic en los conmutadores correspondientes para activar o desactivar.

Si utiliza Microsoft Outlook o Thunderbird, puede configurar los filtros locales antispam directamente en su cliente de correo. Haga clic en el botón **Ajustes** en la barra antispam de Bitdefender (normalmente se encuentra en la parte superior de la ventana del cliente de correo) y, a continuación, en la pestaña **Filtro antispam**.

Configurando la configuración de la nube

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

La protección en la nube funciona mientras tenga activado el Antispam de Bitdefender.

Puede que se envíen a Bitdefender Cloud muestras de mensajes de correo electrónico legítimos o de spam si indica errores de detección o

mensajes de spam que no se hayan detectado. Esto ayuda a mejorar la detección antispam de Bitdefender.

Configure el envío de muestras de mensajes de correo electrónico a Bitdefender Cloud seleccionando las opciones deseadas siguiendo los pasos que se exponen a continuación:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTISPAM** panel, haga clic **Ajustes**.
3. Ve a la **Ajustes** y haga clic en los interruptores de encendido o apagado correspondientes.

Si utiliza Microsoft Outlook o Thunderbird, puede configurar la detección en la nube directamente en su cliente de correo. Haga clic en el botón ⚙ **Ajustes** en la barra antispam de Bitdefender (normalmente se encuentra en la parte superior de la ventana del cliente de correo) y, a continuación, en la pestaña **Configuración en la nube**.

3.2.5. Cortafuego

El cortafuego protege su dispositivo frente a intentos de conexión no autorizados internos y externos, tanto en la red local como en Internet. Es algo parecido a tener un guardia en su puerta: vigila los intentos de conexión a Internet y decide cuáles autorizar y cuáles bloquear.

El cortafuego de Bitdefender usa un conjunto de reglas para filtrar los datos transmitidos desde y hacia su sistema.

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.

Como medida de seguridad, se le notificará cada vez que se bloquee el acceso a Internet de una aplicación potencialmente maliciosa.

Bitdefender asigna automáticamente un tipo de red a cada conexión de red que detecta. Dependiendo del tipo de red, la protección del cortafuego se ajusta al nivel apropiado para cada conexión.

Para obtener más información sobre la configuración del cortafuego para cada tipo de red y cómo editar los ajustes de la red, consulte Administración de ajustes de conexión (página 65).

Activar o desactivar la protección del cortafuego

Para activar o desactivar la protección del cortafuego, haga lo siguiente:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **CORTAFUEGO**, active o desactive el conmutador.

> **Aviso**
> Apagar el cortafuego solo debe hacerse como medida temporal, ya que expondría el dispositivo a conexiones no autorizadas. Vuelva a activar el cortafuego en cuanto sea posible.

Administración de las reglas de aplicaciones

Para ver y administrar las reglas del cortafuego que controlan el acceso de las aplicaciones a los recursos de red y a Internet:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el panel **CORTAFUEGO**, haga clic en **Ajustes**.
3. Acceda a la ventana **Acceso de aplicaciones**.

Puede ver los últimos programas (procesos) que han pasado por el cortafuego de Bitdefender y la red de Internet a la que está conectado. Para ver las reglas creadas para una aplicación concreta, simplemente haga clic en ella y, a continuación, haga clic en el enlace **Ver reglas de aplicaciones**. Se abre la ventana **Reglas**.

Para cada regla se mostrará la siguiente información:

- **RED**: El proceso y tipos de adaptadores de red (Hogar/Oficina, Público o Todos) 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 al que se aplica la regla. De forma predeterminada, las reglas se aplican a todos los protocolos.

- **TRÁFICO**: La regla se aplica en ambas direcciones (entrante y saliente).
- **PORTS**: El protocolo de puerto al que se aplica la regla. Por defecto, las reglas se aplican a todos los puertos.
- **IP**: El protocolo de Internet (IP) al que se aplica la regla. Por defecto, las reglas se aplican a todas las direcciones IP.
- **ACCESO**: Indica si la aplicación tiene acceso o no a la red o a Internet bajo las circunstancias especificadas.

Para editar o eliminar las reglas para la aplicación seleccionada, haga clic en el icono ⋯ .

- **Editar regla**: Abre una ventana donde puede modificar la regla actual.
- **Eliminar regla**: Abre una ventana donde puede optar por eliminar el conjunto actual de reglas para la app seleccionada.

Añadir reglas de apps

Para añadir una regla de app:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **CORTAFUEGOS** panel, haga clic **Ajustes**.
3. En la ventana **Reglas**, haga clic en **Añadir regla**.

Aquí puede aplicar los siguientes cambios:

- **Aplicar esta regla a todas las aplicaciones.** Habilite este conmutador para aplicar la regla que ha creado a todas las aplicaciones.
- **Ruta del programa.** Haga clic en **EXAMINAR** y seleccione la aplicación a la que se aplica la regla.
- **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.
Denegar	Se bloqueará el acceso de la aplicación especificada a la red / Internet bajo las condiciones indicadas.

- **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
Cualquier red	Permitir todo el tráfico entre su dispositivo y otros dispositivos sin importar el tipo de red.
Hogar/Oficina	Permita todo el tráfico entre su dispositivo y los demás en la red local.
Pública	Se filtrará todo el tráfico.

- **Protocolo.** Seleccione en el menú el protocolo IP al que se aplicará 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 ICMP, seleccione **ICMP**.
  - Si desea que la regla se aplique a IGMP, seleccione **IGMP**.
  - Si desea que la regla se aplique a GRE, seleccione **GRE**.
  - 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 del protocolo IP los asigna la Internet Assigned Numbers Authority (IANA). Puede consultar la lista completa de números del protocolo IP asignados en http://www.iana.org/assignments/protocol-numbers.

- **Dirección.** Seleccione en el menú la dirección del tráfico al 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.

Haga clic en el botón **Ajustes avanzados** en la parte inferior de la ventana para personalizar los siguientes ajustes:

- **Dirección local personalizada.** Indique la dirección IP local y el puerto a los que aplicará la regla.
- **Dirección remota personalizada.** Indique la dirección IP remota y el puerto a los que aplicará la regla.

Para eliminar el conjunto actual de reglas y restaurar las predeterminadas, haga clic en **Reiniciar reglas** en la ventana **Reglas**.

Administración de ajustes de conexión

Ya se conecte a Internet por Wi-Fi o mediante un adaptador Ethernet, puede configurar qué ajustes deben aplicarse para una navegación segura. Las opciones entre las que puede elegir son:

- **Dinámico:** El tipo de red se establecerá automáticamente en función del perfil de la red conectada, Hogar/Oficina o Público. Cuando esto sucede, solo se aplican las reglas de cortafuego para el tipo de red concreto o las definidas para aplicar a todos los tipos de red..
- **Hogar/Oficina:** El tipo de red siempre será Hogar/Oficina, sin tener en cuenta el perfil de la red conectada. Cuando esto sucede, solo se aplican las reglas de cortafuego para Hogar/Oficina o las definidas para aplicar a todos los tipos de red..
- **Público:** El tipo de red siempre será Público, sin tener en cuenta el perfil de la red conectada. Cuando esto sucede, solo se aplican las reglas de cortafuego para Público o las definidas para que se apliquen a todos los tipos de red.

Para configurar sus adaptadores de red:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **CORTAFUEGOS** panel, haga clic **Ajustes**.
3. Seleccione la ventana **Adaptadores de red**.
4. Seleccione los ajustes que desee aplicar al conectarse con los siguientes adaptadores:
   - Wi-Fi
   - Ethernet

Configuración de opciones avanzadas

Para configurar los ajustes avanzados del cortafuego:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **CORTAFUEGOS** panel, haga clic **Ajustes**.
3. Selecciona el **Ajustes** ventana.

Pueden configurarse las siguientes características:

- **Protección del análisis de puertos:** 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 dispositivo. Si encuentran un puerto vulnerable o inseguro, pueden intentar entrar en su dispositivo sin su autorización.
- **Modo alertas:** Se muestran alertas cada vez que una aplicación intenta conectarse a Internet. Seleccione **Permitir** o **Bloquear**. Cuando el modo Alertas está activo, la característica **Perfiles** se desactiva automáticamente. El modo Alertas se puede utilizar junto con el **modo Batería**.
- **Permitir el acceso a la red del dominio:** Permite o deniega el acceso a recursos y a recursos compartidos definidos por sus controladores de dominio.
- **Modo Oculto:** Establece si otros dispositivos pueden detectarle. Haga clic en **Editar los ajustes de invisibilidad** para elegir cuándo su dispositivo debe o no estar visible para otros dispositivos.
- **Comportamiento por defecto de la aplicación:** Permite que Bitdefender aplique ajustes automáticos a las aplicaciones sin reglas definidas. Haga clic en **Editar reglas por defecto** para elegir si se deben aplicar o no los ajustes automáticos.
  - Automático: Se permitirá o denegará el acceso a las aplicaciones en función de las reglas automáticas de cortafuego y de usuario.
  - Permitir: Se permitirán automáticamente las aplicaciones que carezcan de una regla de cortafuego definida.
  - Bloquear: Se bloquearán automáticamente las aplicaciones que carezcan de una regla de cortafuego definida.

3.2.6. Vulnerabilidad

Un paso importante para la protección de su dispositivo 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 dispositivo, 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 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 detectar vulnerabilidades del sistema, Bitdefender requiere una conexión a Internet activa.

Para analizar su sistema en busca de vulnerabilidades:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el panel **VULNERABILIDADES**, haga clic en **Abrir**.
3. En la pestaña **Análisis de vulnerabilidades** haga clic en **Iniciar análisis** y, a continuación, espere a que Bitdefender compruebe su sistema para detectar vulnerabilidades. Las vulnerabilidades detectadas se agrupan en tres categorías:
   - **SISTEMA OPERATIVO**
     - **Seguridad del sistema operativo**
       Ajustes alterados del sistema que pueden comprometer su dispositivo y los datos, como no mostrar advertencias cuando los archivos ejecutados realicen cambios en su sistema sin su permiso o cuando dispositivos MTP, como teléfonos o

cámaras, se conecten y ejecuten diferentes operaciones sin su conocimiento.

- **Actualizaciones críticas de Windows**
  Se muestra una lista de las actualizaciones críticas de Windows que no están instaladas en su equipo. Puede que sea necesario reiniciar el sistema para que Bitdefender finalice la instalación. Tenga en cuenta que puede llevar un tiempo instalar las actualizaciones.

- **Cuentas de Windows vulnerables**
  Puede ver la lista de las cuentas de usuario de Windows configuraras en su dispositivo y el nivel de protección de sus contraseñas. Puede elegir entre pedir al usuario que cambie la contraseña en el siguiente inicio de sesión o cambiarla usted mismo inmediatamente. Para establecer una nueva contraseña para su sistema, seleccione **Cambiar la contraseña ahora**.
  Para crear una contraseña segura, le recomendamos que utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como por ejemplo #, $ o @).

- **APLICACIONES**

  - **Seguridad del navegador**
    Cambios en los ajustes de su dispositivo que permiten la ejecución de archivos y programas descargados a través de Internet Explorer sin una validación de integridad, lo que puede comprometer su dispositivo.

  - **Actualización de aplicaciones**
    Para ver información sobre la aplicación que precisa actualizarse, haga clic en su nombre en la lista.
    Si una aplicación no está actualizada, haga clic en el enlace **Descargar una nueva versión** con el fin de descargar la última versión.

- **RED**

  - **Red y credenciales**
    Ajustes alterados del sistema, como conectarse automáticamente a redes de puntos de acceso abiertos sin su

conocimiento o no imponer el cifrado del tráfico saliente del canal seguro.

- **Routers y redes Wi-Fi**
  Para obtener más información sobre la red inalámbrica y el router al que está conectado, haga clic en su nombre en la lista. Si se recomienda establecer una contraseña más segura para su red doméstica, asegúrese de seguir nuestras instrucciones para que pueda permanecer conectado sin preocuparse por su privacidad.
  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.

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. Hacer clic **Notificaciones** en el menú de navegación 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 app está obsoleta, haga clic en **Actualizar ahora** para encontrar un enlace a la página web del proveedor desde donde pueda instalar su última versión.
   - 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 su sistema, haga clic en **Cambiar ajustes de Wi-Fi**.

Para configurar los ajustes de la monitorización de vulnerabilidades:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **VULNERABILIDAD** panel, haga clic **Abierto**.

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

3. Acceda a la pestaña **Ajustes**.
4. Elija las vulnerabilidades del sistema que quiere comprobar regularmente usando los conmutadores correspondientes.
   Actualizaciones 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 de usuario
   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 @).

Reproducción automática

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 amenazas 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.

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.

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

- **Redes Wi-Fi domésticas**
- **Redes Wi-Fi empresariales**
- **Redes Wi-Fi públicas**

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

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

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **VULNERABILIDAD** panel, haga clic **Abierto**.
3. Acceda a la ventana **Ajustes** y active o desactive la opción **Asesor de seguridad Wi-Fi**.

Configurar una red Wi-Fi doméstica

Para empezar a configurar su red doméstica:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **VULNERABILIDAD** panel, haga clic **Abierto**.
3. Acceda a la ventana **Asesor de seguridad Wi-Fi** y haga clic en **Wi-Fi doméstica**.
4. En la pestaña **Wi-Fi doméstica**, haga clic en **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**.

Para añadir una nueva red inalámbrica como doméstica, haga clic en **Seleccionar nueva red Wi-Fi doméstica**.

Configurar una red Wi-Fi empresarial

Para empezar a configurar su red empresarial:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **VULNERABILIDAD** panel, haga clic **Abierto**.
3. Acceda a la ventana **Asesor de seguridad Wi-Fi** y haga clic en **Wi-Fi empresarial**.
4. En la pestaña **Wi-Fi empresarial**, haga clic en **SELECCIONAR WI-FI EMPRESARIAL**.
   Se muestra una lista con las redes inalámbricas a las que se ha conectado hasta ahora.
5. Elija su red empresarial y, a continuación, haga clic en **SELECCIONAR**.

Si una red empresarial 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 empresarial, haga clic en **ELIMINAR**.

Para añadir una nueva red inalámbrica como empresarial, haga clic en **Seleccionar nueva red Wi-Fi empresarial**.

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 Defensa Contra Amenazas Avanzadas
- Se activan los siguientes ajustes de la Prevención de amenazas online:
  - Análisis de sitios web cifrados
  - 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. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **VULNERABILIDAD** panel, haga clic **Abierto**.
3. Acceda a la ventana **Asesor de seguridad Wi-Fi**.
4. En función de la información que necesite, seleccione una de las tres pestañas: **Wi-Fi doméstica**, **Wi-Fi empresarial** o **Wi-Fi pública**.
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 **Ver detalles** del apartado de cada red, se mostrará la siguiente información:

- **Protegida** - aquí puede ver si la red seleccionada está protegida 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.

3.2.7. Protección de vídeo y audio

Cada vez hay más amenazas diseñadas para acceder a las cámaras web y micrófonos integrados. Para evitar el acceso no autorizado a su cámara web e informarse de qué aplicaciones que no son de fiar acceden al micrófono de su dispositivo y cuándo lo hacen, la protección de vídeo y audio de Bitdefender incluye lo siguiente:

- **Protección de cámaras web**
- **Monitor de micrófono**

Protección de cámaras web

Que los piratas informáticos pueden apoderarse de su cámara web para espiarle no es una novedad, y las soluciones para protegerle, como la revocación de los privilegios de las aplicaciones, la desactivación de la cámara integrada del dispositivo, o sencillamente taparla, no son muy prácticas. Para evitar los intentos de vulneración de su privacidad, la Protección de cámaras web de Bitdefender monitoriza permanentemente las aplicaciones que intentan acceder a su cámara, y bloquea aquellas que no sean de fiar.

Como medida de seguridad, se le notificará cada vez que una app que no sea de fiar intente acceder a su cámara.

Activación y desactivación de la Protección de cámaras web

1. Haga clic en **Privacidad** en el menú de navegación de la **interfaz de Bitdefender**.
2. En el panel **PROTECCIÓN DE VÍDEO Y AUDIO**, haga clic en **Ajustes**.
3. Ahora, acceda a la ventana **Ajustes** y active o desactive el conmutador correspondiente.

Configuración de la Protección de cámaras web

Puede configurar qué reglas deben aplicarse cuando una app intente acceder a su cámara siguiendo estos pasos:

1. Hacer clic **Privacidad** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **PROTECCIÓN DE VIDEO Y AUDIO** panel, haga clic **Ajustes**.
3. Ve a la **Ajustes** pestaña.

Tiene las siguientes opciones a su disposición:

Reglas de bloqueo de aplicaciones

- **Bloquear todos los accesos a la cámara web** - No se permitirá a ninguna aplicación acceder a su cámara web.
- **Bloquear el acceso del navegador a la cámara web:** No se permitirá el acceso a su cámara web a ningún navegador web, excepto Internet Explorer y Microsoft Edge. Como las aplicaciones de la Tienda Windows se ejecutan en un único proceso, Bitdefender no puede identificar a Internet Explorer y Microsoft Edge como navegadores web y, por lo tanto, quedan excluidos de este ajuste.
- **Establecer los permisos de aplicaciones según la elección de los usuarios:** Si la mayoría de los usuarios de Bitdefender considera que una aplicación popular es inofensiva, entonces su acceso a la cámara web se fijará automáticamente en Permitir. Si muchos usuarios consideran peligrosa una app popular, entonces su acceso se fijará automáticamente en Bloqueado.

Notificaciones

- **Notificar cuando las aplicaciones permitidas se conecten a la cámara web:** Se le notificará siempre que una app permitida acceda a su cámara web.

Añadir apps a la lista de Protección de cámaras web

Las apps que intentan conectarse a su cámara web se detectan automáticamente y, dependiendo de su comportamiento y de la elección de la comunidad, se les permite o no su acceso. No obstante, puede determinar manualmente por su cuenta la acción que debe adoptarse siguiendo estos pasos:

1. Hacer clic **Privacidad** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **PROTECCIÓN DE VIDEO Y AUDIO** panel, haga clic **Ajustes**.
3. Acceda a la ventana **Protección de cámaras web**.
4. Haga clic en la ventana **Añadir aplicación**.
5. Haga clic en el enlace que desee:
   - **Desde la Tienda Windows:** Muestra una lista con las aplicaciones de la Tienda Windows detectadas. Active los conmutadores junto a las apps que desee añadir a la lista.
   - **Desde sus aplicaciones:** Vaya al archivo .exe que desea añadir a la lista y, a continuación, haga clic en **Aceptar**.

Para ver lo que los usuarios de Bitdefender han decidido hacer con la aplicación seleccionada, haga clic en el icono .

En esta ventana aparecerán las apps que soliciten acceso a su cámara, junto con la hora de su última actividad.

Se le notificará cada vez que una de las apps permitidas resulte bloqueada por los usuarios de Bitdefender.

Para interrumpir el acceso a su cámara web de una aplicación añadida, haga clic en el icono .

El icono pasa a , lo que significa que la aplicación seleccionada no tendrá acceso a su cámara web.

Monitor de micrófono

Las aplicaciones fraudulentas pueden acceder al micrófono incorporado, secretamente o en segundo plano, sin su consentimiento. Para informarle sobre posibles ataques maliciosos, el Monitor de micrófono de Bitdefender le avisará en tales circunstancias. Así, ninguna aplicación podrá acceder a su micrófono sin que usted lo sepa.

Activar o desactivar el Monitor de micrófono

1. Hacer clic **Privacidad** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **PROTECCIÓN DE VIDEO Y AUDIO** panel, haga clic **Ajustes**.
3. Selecciona el **Ajustes** ventana.
4. En la ventana **Ajustes**, active o desactive el conmutador de **Monitor de micrófono**.

Configuración de notificaciones para el Monitor de micrófono

Para configurar qué notificaciones deben aparecer cuando las aplicaciones intenten acceder a su micrófono, siga los pasos que se exponen a continuación:

1. Hacer clic **Privacidad** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **PROTECCIÓN DE VIDEO Y AUDIO** panel, haga clic **Ajustes**.
3. Ve a la **Ajustes** ventana.

Notificaciones

- **Notificar cuando una aplicación intente acceder al micrófono**
- **Notificar cuando los navegadores accedan al micrófono**
- **Notificar cuando las aplicaciones que no sean de confianza accedan al micrófono**
- **Mostrar notificación según la elección de los usuarios de Bitdefender**

Añadir aplicaciones a la lista del Monitor de micrófono

Las aplicaciones que intenten conectarse a su micrófono se detectarán automáticamente y se añadirán a la lista de notificaciones. No obstante,

puede configurar manualmente por su cuenta si debe mostrarse una notificación siguiendo los pasos que se exponen a continuación:

1. Hacer clic **Privacidad** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **PROTECCIÓN DE VIDEO Y AUDIO** panel, haga clic **Ajustes**.
3. Acceda a la ventana **Protección de audio**.
4. Hacer clic **Agregar aplicación** ventana.
5. Haga clic en el enlace deseado:
   - **Desde la tienda de Windows** - Se muestra una lista con las aplicaciones de la Tienda Windows detectadas. Encienda los interruptores junto a las aplicaciones que desea agregar a la lista.
   - **Desde tus aplicaciones** - vaya al archivo .exe que desea agregar a la lista y luego haga clic en **DE ACUERDO**.

Para ver lo que los usuarios de Bitdefender han elegido hacer con la aplicación seleccionada, haga clic en el botón icono.

En esta ventana aparecerán las aplicaciones que soliciten acceso a su micrófono, junto con la hora de su última actividad.

Para dejar de recibir notificaciones sobre la actividad de una aplicación añadida, haga clic en el icono.

El icono pasa a, lo que significa que no se mostrará ninguna notificación de Bitdefender cuando la aplicación seleccionada intente acceder a su micrófono.

3.2.8. Reparación de ransomware

La Reparación de ransomware de Bitdefender realiza una copia de seguridad de sus archivos, como documentos, imágenes, vídeos o música, para asegurarse de que estén protegidos contra daños o pérdida en caso de que un ransomware los cifre. Si se detecta un ataque de ransomware, Bitdefender bloqueará todos los procesos implicados en el ataque y comenzará el proceso de reparación. De esta forma, podrá recuperar todo el contenido de sus archivos sin pagar ningún rescate.

Activación y desactivación de la Reparación de ransomware

Para activar y desactivar la Reparación de ransomware:

1. 1. Haga clic en **Protección** en el menú de navegación de la **interfaz de Bitdefender**.
2. En el panel **REPARACIÓN DE RANSOMWARE**, active o desactive el conmutador.

> **Nota**
> Para asegurarse de que sus archivos estén protegidos contra el ransomware, le recomendamos que mantenga habilitada la Reparación de ransomware.

Activar o desactivar la restauración automática

La restauración automática se asegura de que sus archivos se restauren automáticamente en caso de que un ransomware los cifre.

Para activar o desactivar la restauración automática:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el panel **REPARACIÓN DE RANSOMWARE**, haga clic en **Administrar**.
3. En la ventana Ajustes, active o desactive el conmutador **Restauración automática**.

Visualización de archivos que se restauraron automáticamente

Cuando se habilita la opción **Restauración automática**, Bitdefender restaura automáticamente los archivos que un ransomware pudiera cifrar. Así, puede usar su dispositivo sin preocupaciones, sabiendo que sus archivos están a salvo.

Para ver archivos que se restauraron automáticamente:

1. Hacer clic **Notificaciones** en el menú de navegación de la Interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación del último comportamiento de ransomware reparado y luego haga clic en **Archivos restaurados**.
   Se muestra la lista con los archivos restaurados. Aquí también puede ver la ubicación donde se restauraron sus archivos.

Restaurar manualmente archivos cifrados

En caso de tener que restaurar manualmente los archivos que resultaron cifrados, siga los pasos que se exponen a continuación:

1. Hacer clic **Notificaciones** en el menú de navegación de la Interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación del último comportamiento de ransomware detectado y luego haga clic en **Archivos cifrados**.
3. Se muestra la lista con los archivos cifrados.
   Haga clic en **Recuperar archivos** para continuar.
4. En caso de que la totalidad o una parte del proceso de restauración falle, debe elegir la ubicación donde se guardarán los archivos descifrados. Haga clic en **Restaurar ubicación** y luego elija una en su PC.
5. Aparecerá una ventana de confirmación.
   Haga clic en **Finalizar** para terminar el proceso de restauración.

En caso de cifrado, se pueden restaurar los archivos con las siguientes extensiones:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com ; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

Añadir aplicaciones a excepciones

Puede configurar reglas de excepción para las apps de confianza, de modo que la característica de Reparación de ransomware no las bloquee si realizan acciones típicas del ransomware.

Para añadir apps a la lista de excepciones de la Reparación de ransomware:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.

2. En el **REMEDIACIÓN DE RANSOMWARE** panel, haga clic **Administrar**.
3. Acceda a la ventana **Excepciones** y haga clic en **+Añadir una excepción**.

3.2.9. Cryptomining Protection

¿Qué es la protección contra la criptominería?

Con el uso de criptominería, los atacantes pueden beneficiarse financieramente sin asumir los costos y consecuencias legales asociados.

La función Cryptomining Protection de Bitdefender defiende las computadoras con Windows contra la creciente amenaza de actividades no autorizadas de criptominería, una práctica maliciosa que explota los recursos y la electricidad de un usuario para generar ingresos para los atacantes.

> **Nota**
> La protección de criptominería se basa en:
>
> - Escudo de Bitdefender
> - Prevención de ataques web
>
> Para que Cryptomining Protection pueda ejecutarse, estas dos funciones también deben estar habilitadas.

Habilitación de la protección contra la criptominería

La función Protección de criptominería se encuentra dentro de la pestaña Protección.

Para habilitarlo, simplemente active su interruptor correspondiente.

> **Nota**
> La protección contra criptominería está desactivada de forma predeterminada, lo que garantiza que los usuarios tengan control sobre su activación.

Modos de operacion

Una vez habilitada, la función Cryptomining Protection opera en 2 estados distintos, cada uno adaptado a las preferencias del usuario:

1. **Bloquea todas las actividades de Cryptomining.** (bloquea automáticamente cualquier actividad de criptominería y toma las medidas necesarias para evitar futuros intentos no autorizados)
   Este modo es ideal para usuarios que no tienen intención de participar en actividades de criptominería.
2. **Detectar actividades de Criptominería.** (emite alertas cada vez que se detecta una actividad de criptominería y requiere la participación del usuario para determinar la acción apropiada)
   Este modo es adecuado para usuarios que participan activamente en sus propias actividades de criptominería pero que desean monitorear y controlar cualquier intento no autorizado.

Administrar excepciones

Se pueden especificar excepciones para aplicaciones, con la capacidad adicional de definir líneas de comando específicas. Sin embargo, también se pueden establecer excepciones sin necesidad de proporcionar parámetros tan detallados, ofreciendo un equilibrio entre personalización y simplicidad.

Para agregar una excepción:

1. Hacer clic**Proteccion**en el menú del lado izquierdo de la interfaz de Bitdefender.
2. En el**Protección de criptominería**panel, haga clic en**Ajustes**.
3. Haga clic en el**Administrar excepciones**opción.
4. A continuación, haga clic en**Agregar una excepción**botón.
5. Una nueva ventana se abrirá. Puede excluir manualmente aplicaciones, URL y direcciones IP.
6. Finalmente, haga clic**Ahorrar**. La nueva regla se agrega a la lista de excepciones de Protección Cryptomining.

> **Nota**
> Para eliminar una excepción, simplemente haga clic en el icono de la papelera que se encuentra junto a ella.

3.2.10. Anti-tracker

Muchos sitios web que visita utilizan rastreadores para recopilar información sobre su comportamiento, ya sea para compartirla con

empresas de terceros o para mostrarle anuncios más relevantes para usted. De esta forma, los propietarios de sitios web obtienen dinero para poder brindarle contenidos gratuitos o seguir operando. Además de recopilar información, los rastreadores pueden ralentizar su navegación o desperdiciar su ancho de banda.

Con la extensión Bitdefender Anti-tracker activada en su navegador evita que le rastreen, para mantener la privacidad de sus datos mientras navega y acelerar el tiempo de carga de los sitios web.

La extensión de Bitdefender es compatible con los siguientes navegadores:

- explorador de Internet
- Google Chrome
- Mozilla Firefox

Los rastreadores que detectamos se agrupan en las siguientes categorías:

- **Publicidad**: Se utilizan para analizar el tráfico del sitio web, el comportamiento de los usuarios o los patrones de tráfico de los visitantes.
- **Interacción con el cliente**: Se utilizan para medir la interacción del usuario con diferentes sistemas de entrada, como pueden ser un chat o un formulario de soporte.
- **Esencial**: Se utilizan para monitorizar las funciones críticas de la página web.
- **Análisis del sitio**: Se utilizan para recopilar datos sobre el uso de la página web.
- **Redes sociales**: Se utilizan para monitorizar la audiencia, actividad e interacción del usuario con diferentes plataformas de redes sociales.

Interfaz de Anti-tracker

Cuando se activa la extensión Bitdefender Anti-tracker, aparece el icono junto a la barra de búsqueda en su navegador. Cada vez que visita un sitio web, puede observar un contador en el icono, que hace referencia a los rastreadores detectados y bloqueados. Para ver más información sobre los rastreadores bloqueados, haga clic en el icono para abrir la interfaz. Además del número de rastreadores bloqueados, puede ver el tiempo necesario para cargar la página y las categorías a las que

pertenecen los rastreadores detectados. Para ver la lista de sitios web que le están rastreando, haga clic en la categoría deseada.

Para que Bitdefender deje de bloquear los rastreadores del sitio web que visita actualmente, haga clic en **Pausar la protección en este sitio web**. Este ajuste solo se aplica mientras tenga abierto el sitio web y se revertirá a su estado inicial cuando lo cierre.

Para permitir a los rastreadores de determinada categoría monitorizar su actividad, haga clic en la actividad deseada y luego en el botón correspondiente. Si cambia de parecer, haga clic nuevamente en el mismo botón.

Desactivación de Bitdefender Anti-tracker

Para desactivar Bitdefender Anti-tracker:

- Desde su navegador web:
  1. Abra su navegador Web.
  2. Haga clic en el icono junto a la barra de direcciones de su navegador.
  3. Haga clic en el icono en la esquina superior derecha.
  4. Utilice el conmutador correspondiente para desactivarlo.
     El icono de Bitdefender se vuelve gris.
- Desde lainterfaz de Bitdefender:
  1. Hacer clic **Privacidad** en el menú de navegación de la Interfaz de Bitdefender.
  2. En el panel **ANTI-TRACKER**, haga clic en **Ajustes**.
  3. Junto al navegador para el que desea inhabilitar la extensión, desactive el conmutador correspondiente.

Permitir el rastreo de un sitio web

Si desea que se le rastree cuando visita determinado sitio web, puede añadir su dirección a las excepciones de la siguiente manera:

1. Abre tu navegador web.
2. Haga clic en el icono junto a la barra de búsqueda.

3. Haga clic en el icono en la esquina superior derecha.
4. Si se encuentra en el sitio web que desea añadir a las excepciones, haga clic en **Añadir el sitio web actual a la lista**.
   Si desea añadir otro sitio web, escriba su dirección en el campo correspondiente y, a continuación, haga clic en .

3.2.11. 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 por Internet y cualquier otro tipo de transacción en la Red.

Bitdefender Safepay™ ofrece las siguientes características:

- Bloquea el acceso a su escritorio y cualquier intento de tomar capturas de su pantalla.
- 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 dispositivo 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 la banca electrónica y las compras por Internet; con Bitdefender Safepay puede abrir cualquier sitio web™.

Uso de Bitdefender Safepay™

Por omisión, Bitdefender detecta cuando navega hacia una página de un banco o una tienda online en cualquier navegador de su dispositivo 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. Hacer clic **Privacidad** en el menú de navegación de la Interfaz de Bitdefender.
  2. En el panel **SAFEPAY**, haga clic en **Ajustes**.
  3. En la ventana **Safepay**, haga clic en **Lanzar 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™" directamente en la pantalla de Inicio) y luego haga clic en el icono.
  - En **Windows 10** y **Windows 11**:
    Escriba "Bitdefender Safepay™" en el cuadro de búsqueda de la barra de tareas y haga clic en su icono.

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 varios sitios web en la ventana de Bitdefender Safepay™ haciendo clic en ⊞.

- Navegue hacia atrás y hacia delante y refresque las páginas usando ← → ↻ respectivamente.
- Acceda a los **ajustes** de Bitdefender Safepay™ haciendo clic y seleccionando **Ajustes**.
- Gestione sus **marcadores** haciendo clic en ☆, junto a la barra de direcciones.
- Abra el teclado virtual haciendo clic en .
- Aumente o disminuya el tamaño del navegador pulsando simultáneamente **Ctrl** y las teclas **+/-** del teclado numérico.
- Vea la información acerca de su producto Bitdefender haciendo clic en ⋯ y seleccionando **Acerca de**.
- Imprima información importante haciendo clic en ⋯ y eligiendo **Imprimir**.

> **Nota**
> Para cambiar entre el Escritorio de Windows y Bitdefender Safepay™, pulse las teclas **Alt+Tab** o haga clic en la opción **Cambiar a Escritorio** de la esquina superior izquierda de la ventana.

Configuración de ajustes

Haga clic en ⋯ y seleccione **Ajustes** para configurar Bitdefender Safepay™:

Aplicar las reglas de Bitdefender Safepay a los dominios a los que se acceda

Aquí aparecerán los sitios web que haya añadido a **Marcadores** con la opción **Abrir automáticamente en Safepay** habilitada. Si desea dejar de abrir automáticamente con Bitdefender Safepay™ un sitio web de la lista, haga clic en × junto a la entrada deseada de la columna **Eliminar**.

Bloquear 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.

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.

Haga clic en **IMPORTAR** y siga el asistente para utilizar los certificados en Bitdefender Safepay™.

Usar el teclado virtual

Cuando seleccione un campo de contraseña, aparecerá automáticamente el teclado virtual.

Utilice el conmutador correspondiente para activar o desactivar la función.

Confirmación de impresión

Active esta opción si desea dar su confirmación antes de que comience el proceso de impresión.

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 ⋯ y seleccione **Marcadores** 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. Escriba la URL y el título del marcador y, a continuación, 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.

Desactivar las notificaciones de Safepay

El producto Bitdefender está configurado para que le notifique, mediante una ventana emergente, cuando detecte un sitio de banca.

Para desactivar las notificaciones de Safepay:

1. Hacer clic **Privacidad** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **SEGURIDAD** panel, haga clic **Ajustes**.
3. En la ventana **Ajustes**, desactive el conmutador junto a **Notificaciones de Safepay**.

3.2.12. dispositivo antirrobo

El robo de computadoras portátiles es un problema importante que afecta a individuos y organizaciones por igual. Incluso más que perder el hardware en sí, los datos que se pierden con él pueden causar daños significativos, tanto económicos como emocionales.

Sin embargo, pocas personas toman las medidas adecuadas para proteger sus importantes datos personales, comerciales y financieros en caso de robo o pérdida.

Bitdefender Anti-Theft lo ayuda a estar mejor preparado para tal evento al permitirle ubicar o bloquear su computadora portátil de forma remota e incluso borrar todos los datos, en caso de que alguna vez se separe de su computadora portátil en contra de su voluntad.

Para utilizar las funciones de Anti-Theft, se deben cumplir los siguientes requisitos previos:

- Los comandos solo se pueden enviar desde la cuenta de Bitdefender.
- La computadora portátil debe estar conectada a Internet para recibir los comandos.

Las funciones antirrobo funcionan de la siguiente manera:

Localizar

Vea la ubicación de su dispositivo en Google Maps.

La precisión de la ubicación depende de cómo Bitdefender pueda determinarla. La ubicación se determina dentro de decenas de metros si Wi-Fi está habilitado en su computadora portátil y hay redes inalámbricas en su rango.

Si la computadora portátil está conectada a una LAN con cable sin una ubicación basada en Wi-Fi disponible, la ubicación se determinará en función de la dirección IP, que es considerablemente menos precisa.

Alerta

Envía una alerta remota en el dispositivo.

La función solo está disponible en dispositivos móviles.

Cerrar

Bloquee su computadora portátil y configure un PIN de 4 dígitos para desbloquearla. Cuando envías el **Cerrar** comando, el sistema se reinicia y solo es posible volver a iniciar sesión en Windows después de ingresar el PIN que configuró.

Si desea que Bitdefender tome fotos de quien intente acceder a su computadora portátil, marque la casilla de verificación correspondiente. Las fotos tomadas se toman con la cámara frontal y se muestran junto con la marca de tiempo en el tablero de Anti-Theft. Solo se guardarán las dos fotos más recientes.

Esta acción está disponible solo para computadoras portátiles que tienen cámara frontal.

Limpiar

Elimina todos los datos de tu sistema. Cuando envías el **Limpiar** comando, la computadora portátil se reinicia y los datos en todas las particiones del disco duro se borran.

Mostrar IP

Muestra la última dirección IP del dispositivo seleccionado. Hacer clic **MOSTRAR IP** para hacerlo visible.

Anti-Theft se activa después de la instalación y se puede acceder exclusivamente a través de su cuenta de Bitdefender desde cualquier dispositivo conectado a Internet, en cualquier lugar.

Uso de funciones antirrobo

Para acceder a las funciones de Antirrobo, utilice una de las siguientes posibilidades:

- Desde la interfaz principal de Bitdefender:
  1. Hacer clic **Utilidades** en el menú de navegación en el Interfaz de Bitdefender.
  2. Hacer clic **IR AL CENTRO**.
     Se le redirigirá a la página de Bitdefender Central. Asegúrese de haber iniciado sesión con sus credenciales.
  3. En la ventana de Bitdefender Central que se abre, haga clic en la tarjeta del dispositivo deseado, luego seleccione **Anti-robo**.
- En cualquier dispositivo con acceso a internet:
  1. Abra un navegador web y vaya a: https://central.bitdefender.com.
  2. Inicie sesión en su cuenta de Bitdefender con su dirección de correo electrónico y contraseña.
  3. Selecciona el **Mis dispositivos** panel.
  4. Haga clic en la tarjeta del dispositivo deseado, luego seleccione **Anti-robo**.
  5. Seleccione la función que desea utilizar:
     Localizar - mostrar la ubicación de su dispositivo en Google Maps.
     Mostrar IP - mostrar la última dirección IP de su dispositivo.
     Alerta - enviar una alerta en el dispositivo.
     Cerrar - Bloquee su computadora portátil y establezca un código PIN para desbloquearla.
     Limpiar - elimine todos los datos de su computadora portátil.

     > **Importante**
     > Después de borrar un dispositivo, todas las funciones antirrobo dejan de funcionar.

3.3. Utilidades

3.3.1. 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 la película
- Perfil del juego
- **Perfil de redes Wi-Fi públicas**
- Perfil de modo de 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.
- El **Asesor de búsquedas** está inhabilitado.
- Las notificaciones de ofertas especiales 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:

- Advanced Threat Defense está activado
- Las siguientes configuraciones de Prevención de amenazas en línea están activadas:
  - Escaneo web encriptado
  - Protección contra el fraude
  - Protección contra el 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. Hacer clic **Utilidades** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **Perfiles** pestaña, haga clic **Ajustes**.
3. Haga clic en el botón **CONFIGURAR** del área del Perfil de trabajo.
4. 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

5. Haga clic en **GUARDAR** para aplicar los cambios y cierre 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 app de trabajo, puede añadirla manualmente a la **Lista de aplicaciones de trabajo**.

Para añadir apps manualmente a la Lista de aplicaciones de trabajo en el Perfil de trabajo:

1. Hacer clic **Utilidades** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **Perfiles** pestaña, haga clic **Ajustes**.
3. Haga clic en el **CONFIGURAR** del área Perfil de trabajo.
4. En la ventana **Ajustes del perfil de trabajo**, haga clic en **Lista de aplicaciones**.
5. Haga clic en **AÑADIR**.
   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. Hacer clic **Utilidades** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **Perfiles** pestaña, haga clic **Ajustes**.

3. Haga clic en el botón **CONFIGURAR** del área del Perfil de películas.
4. Elija los ajustes del sistema que le gustaría que se aplicaran marcando las siguientes opciones:
   - Aumentar el rendimiento en reproductores de vídeo
   - Optimizar los ajustes del producto para el perfil de Películas
   - Posponer programas en segundo plano y tareas de mantenimiento
   - Posponer actualizaciones automáticas de Windows
   - Ajustar el plan de energía para películas
5. Hacer clic **AHORRAR** 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 app de reproducción de vídeo, puede añadirla manualmente a la **Lista de aplicaciones de películas**.

Para añadir reproductores de vídeo manualmente a la Lista de aplicaciones de películas en el Perfil de películas:

1. Hacer clic **Utilidades** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **Perfiles** pestaña, haga clic **Ajustes**.
3. Haga clic en el **CONFIGURAR** del área Perfil de película.
4. En la ventana **Ajustes del perfil de películas**, haga clic en **Lista de reproductores**.
5. Hacer clic **AGREGAR**.
   Aparece una nueva ventana. Busque el archivo ejecutable de la aplicación, selecciónelo y haga clic en **DE ACUERDO** para agregarlo 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. Hacer clic **Utilidades** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **Perfiles** pestaña, haga clic **Ajustes**.
3. Haga clic en el botón **Configurar** del área del Perfil de juego.
4. Elija los ajustes del sistema que le gustaría que se aplicaran marcando las siguientes opciones:
   - Aumentar el rendimiento en los juegos
   - Optimizar los ajustes del producto para el perfil de Juego
   - Posponer programas en segundo plano y tareas de mantenimiento
   - Posponer actualizaciones automáticas de Windows
   - Ajustar el plan de energía para juegos
5. Hacer clic **AHORRAR** 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 app, puede añadirlo manualmente a la {1}Lista de aplicaciones de juego{2}.

Para añadir juegos manualmente a la Lista de aplicaciones de juego en el Perfil de juego:

1. Hacer clic **Utilidades** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **Perfiles** pestaña, haga clic **Ajustes**.
3. Haga clic en el **Configurar** del área Perfil del juego.
4. En la ventana **Ajustes del perfil de juego**, haga clic en **Lista de juegos**.
5. Hacer clic **AGREGAR**.

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. Hacer clic **Utilidades** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **Perfiles** pestaña, haga clic **Ajustes**.
3. Haga clic en el botón **CONFIGURAR** del área del perfil de redes Wi-Fi públicas.
4. 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**.
5. Hacer clic **Ahorrar**.

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. Hacer clic **Utilidades** en el menú de navegación de la Interfaz de Bitdefender.

2. En el **Perfiles** pestaña, haga clic **Ajustes**.
3. Haga clic en el botón **Configurar** del área del perfil del modo Batería.
4. 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.
5. Hacer clic **AHORRAR** 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.
- Los análisis programados se posponen.

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. Hacer clic **Utilidades** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **Perfiles** pestaña, haga clic **Ajustes**.
3. Desplácese hacia abajo hasta ver la opción de Optimización en tiempo real y, a continuación, utilice el conmutador correspondiente para activarla o desactivarla.

3.3.2. Optimizador de un clic

Problemas como fallas en el disco duro, archivos de registro sobrantes e historial del navegador pueden ralentizar su trabajo, lo que puede volverse molesto para usted. Todo esto ahora se puede arreglar con un solo clic de un botón.

OneClick Optimizer le permite identificar y eliminar archivos inútiles ejecutando múltiples tareas de limpieza al mismo tiempo.

Para iniciar el proceso de OneClick Optimizer:

1. Hacer clic **Utilidades** en el menú de navegación de la Interfaz de Bitdefender.
2. Haga clic en el **Optimizar** botón.
   a. **analizando**
   Espere a que Bitdefender termine de buscar problemas del sistema.
      - Liberador de espacio en disco: identifica archivos y carpetas innecesarios.
      - Limpieza del Registro: identifica referencias no válidas o desactualizadas en el Registro de Windows.
      - Limpieza de privacidad: identifica archivos y cookies temporales de Internet, caché e historial del navegador.

      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. **optimizando**
   Espere a que Bitdefender termine de optimizar su sistema.

   c. **Asuntos**
   Aquí es donde puede ver el resultado de la operación.

Si desea información completa sobre el proceso de optimización, haga clic en el **Ver informe detallado** botón.

3.3.3. Protección de datos

Eliminar archivos de forma permanente

Cuando los usuarios eliminan un archivo, ya no se puede acceder a él por medios normales. Sin embargo, el archivo sigue almacenado en el disco duro hasta que se sobrescribe al copiar nuevos archivos.

Bitdefender File Shredder lo ayuda a eliminar datos de forma permanente al eliminarlos físicamente de su disco duro.

Puede destruir rápidamente archivos y carpetas desde su dispositivo 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. Haga clic en **Eliminar permanentemente** y, a continuación, confirme que desea continuar con el proceso.
   Espere a que Bitdefender termine de destruir los archivos.
4. Los resultados son mostrados. Haga clic en **Finalizar** para salir del asistente.

Como alternativa, puede destruir los archivos desde la interfaz de Bitdefender de la siguiente manera:

1. Hacer clic **Utilidades** en el menú de navegación de la Interfaz de Bitdefender.
2. En el panel **Protección de datos**, haga clic en **Destructor de archivos**.
3. Siga el asistente del Destructor de archivos:
   a. Haga clic en el botón **Añadir carpetas** para añadir los archivos o carpetas que desee eliminar de forma permanente.
      Como alternativa, arrastre los archivos o carpetas a esta ventana.
   b. Haga clic en **Eliminar permanentemente** y, a continuación, confirme que desea continuar con el proceso.

Espere a que Bitdefender termine de triturar los archivos.

c. **Resumen de resultados**
Se muestran los resultados. Hacer clic **Finalizar** para salir del asistente.

3.4. Cómo

3.4.1. Instalación

¿Cómo instalo Bitdefender en un segundo dispositivo?

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

Para instalar Bitdefender en un segundo dispositivo:

1. Haga clic en **Instalar en otro dispositivo** en la esquina inferior izquierda de la **interfaz de Bitdefender**.
Aparece una nueva ventana en su pantalla.
2. Hacer clic **COMPARTIR ENLACE DE DESCARGA**.
3. Siga las instrucciones que aparecen en la pantalla para instalar Bitdefender.

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

¿Cómo puedo reinstalar Bitdefender?

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

- ha reinstalado el sistema operativo.
- desea reparar los problemas que puedan haber causado demoras o cierres inesperados.
- su producto Bitdefender no se inicia o no funciona correctamente.

En caso de que experimente alguna de las situaciones mencionadas, siga los pasos que se exponen a continuación:

- En **ventanas 7**:
    1. Hacer clic **Comenzar** E ir a **Todos los programas**.

2. Busque *Bitdefender Total Security* y seleccione **Desinstalar**.
3. Haga clic en **REINSTALAR** en la ventana que aparece.
4. Necesita reiniciar el dispositivo para completar el proceso.

- En **ventanas 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. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
4. Hacer clic **REINSTALAR** en la ventana que aparece.
5. Debe reiniciar el dispositivo para completar el proceso.

- En **ventanas 10** y **ventanas 11**:

1. Haga clic en **Inicio** y, a continuación, haga clic en **Ajustes**.
2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones y características**.
3. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
4. Haga clic en **Desinstalar** para confirmar su elección.
5. Haga clic en **REINSTALAR**.
6. Debe reiniciar el dispositivo para completar el proceso.

> **Nota**
> Siguiendo este procedimiento de reinstalación, se guardan los ajustes personalizados para que estén disponibles en el nuevo producto instalado. Puede que otros ajustes vuelvan a su valor por defecto.

¿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 dispositivo desde la plataforma de Bitdefender Central.

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

Para instalar Bitdefender desde Bitdefender Central:

1. Acceso Centro de Bitdefender.
2. Selecciona el **Mis dispositivos** panel y, a continuación, haga clic en **INSTALAR PROTECCIÓN**.
3. Elija una de las dos opciones disponibles:
   - **Protege este dispositivo**
     Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
   - **Proteger otros dispositivos**
     Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
     Hacer clic **ENVIAR ENLACE DE DESCARGA**. Escriba una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR CORREO ELECTRÓNICO**. Tenga en cuenta que el enlace de descarga generado es válido solo durante las próximas 24 horas. Si el enlace caduca, deberá generar uno nuevo siguiendo los mismos pasos.
     En el dispositivo en el que desea instalar su producto Bitdefender, verifique la cuenta de correo electrónico que ingresó y luego haga clic en el botón de descarga correspondiente.
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.

Pueden darse dos casos:

- Ha actualizado el sistema operativo utilizando Windows Update y observa que Bitdefender ya no funciona.
  En este caso, necesita reinstalar el producto siguiendo estos pasos:
  - En **ventanas 7**:
    1. Haga clic en **Inicio**, acceda al **Panel de control** y haga doble clic en **Programas y características**.
    2. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
    3. Hacer clic **REINSTALAR** en la ventana que aparece.
    4. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
       Abra la interfaz de su nuevo producto Bitdefender recién instalado para acceder a sus características.
  - En **ventanas 8** y **Windows 8.1**:
    1. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control" directamente en la pantalla de inicio) y luego hacer clic en su icono.
    2. Haga clic en **Desinstalar un programa** o **Programas y características**.
    3. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
    4. Hacer clic **REINSTALAR** en la ventana que aparece.
    5. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.
       Abra la interfaz de su nuevo producto Bitdefender instalado para tener acceso a sus funciones.

- En **ventanas 10** y **ventanas 11**:
  1. Hacer clic **Comenzar**, luego haga clic **Ajustes**.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones**.
  3. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
  4. Hacer clic **Desinstalar** de nuevo para confirmar su elección.
  5. Hacer clic **REINSTALAR** en la ventana que aparece.
  6. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.
     Abra la interfaz de su nuevo producto Bitdefender instalado para tener acceso a sus funciones.

  > **Nota**
  > Al seguir este procedimiento de reinstalación, la configuración personalizada se guarda y está disponible en el nuevo producto instalado. Otros ajustes pueden volver a su configuración predeterminada.

- 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. Acceso Centro de Bitdefender.
     b. Selecciona el **Mis dispositivos** panel y, a continuación, haga clic en **INSTALAR PROTECCIÓN**.
     c. Elija una de las dos opciones disponibles:
        - **Protege este dispositivo**
          Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
        - **Proteger otro dispositivo**
          Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.

Hacer clic **ENVIAR ENLACE DE DESCARGA**. Escriba una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR CORREO ELECTRÓNICO**. Tenga en cuenta que el enlace de descarga generado es válido solo durante las próximas 24 horas. Si el enlace caduca, deberá generar uno nuevo siguiendo los mismos pasos.

En el dispositivo en el que desea instalar su producto Bitdefender, verifique la cuenta de correo electrónico que ingresó y luego haga clic en el botón de descarga correspondiente.

2. Ejecute el producto Bitdefender que ha descargado.

Para obtener más información acerca del proceso de instalación de Bitdefender consulte Instalando su producto Bitdefender (página 18).

¿Cómo puedo actualizar a la última versión de Bitdefender?

Desde ahora, es posible actualizar a la versión más reciente sin seguir el procedimiento manual de desinstalación y reinstalación. Para ser más exactos, el nuevo producto que incluye características nuevas y mejoras importantes se proporciona a través de la actualización del producto y, si ya tiene una suscripción activa a Bitdefender, el producto se activa automáticamente.

Si utiliza la versión 2020, puede actualizar a la última versión siguiendo estos pasos:

1. Haga clic en **REINICIAR AHORA** en la notificación que reciba con la información de actualización. Si la pasa por alto, acceda a la ventana **Notificaciones**, seleccione la actualización más reciente y, a continuación, haga clic en el botón **REINICIAR AHORA**. Espere a que se reinicie el dispositivo.
   Aparece la ventana **Novedades** con información sobre las características nuevas y mejoradas.
2. Haga clic en el enlace **Más información** para leer una página con más detalles y artículos útiles.
3. Cierre la ventana **Novedades** para acceder a la interfaz de la nueva versión instalada.

Los usuarios que deseen actualizar gratuitamente desde Bitdefender 2016 o una versión anterior a la más reciente de Bitdefender, deben eliminar su versión actual del Panel de control y, a continuación, descargar el archivo de instalación más reciente desde el sitio web de Bitdefender en la siguiente dirección: https://www.bitdefender.com/Downloads/. La activación solo es posible con una suscripción válida

3.4.2. Centro de Bitdefender

¿Cómo inicio sesión en la cuenta de Bitdefender con otra cuenta?

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

Para poder iniciar sesión con otra cuenta de Bitdefender:

1. Haga clic en el nombre de su cuenta en la parte superior de la **interfaz de Bitdefender**.
2. Haga clic en **Cambiar cuenta** en la esquina superior derecha de la pantalla para cambiar la cuenta vinculada al dispositivo.
3. Escriba la dirección de correo electrónico en el campo correspondiente y luego haga clic en **PRÓXIMO**.
4. Escriba su contraseña y luego 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 Solicitando Ayuda (página 265).

¿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. Acceso Centro de Bitdefender.

2. Haga clic en el icono en la parte superior derecha de la pantalla.
3. Haga clic en **Mi cuenta** en el menú deslizante.
4. Haga clic en **Ajustes** en el menú deslizante.
5. Inhabilite la opción **Activar o desactivar los mensajes de ayuda**.

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

Hay dos posibilidades para establecer una nueva contraseña para su cuenta de Bitdefender:

- Desde el Interfaz de Bitdefender:
  1. Hacer clic **Mi cuenta** en el menú de navegación de la Interfaz de Bitdefender.
  2. Haga clic en **Cambiar cuenta** en la esquina superior derecha de la pantalla.
     Aparecerá una nueva ventana.
  3. Escriba su dirección de correo electrónico y haga clic en **SIGUIENTE**.
     Aparece una nueva ventana.
  4. Hacer clic **¿Has olvidado tu contraseña?**.
  5. Haga clic en **SIGUIENTE**.
  6. Verifique su cuenta de correo electrónico, escriba el código de seguridad que ha recibido y luego haga clic en **PRÓXIMO**.
     Como alternativa, puede hacer clic en **Cambiar la contraseña** en el correo que te enviamos.
  7. Escriba la nueva contraseña que desea establecer y luego escríbala una vez más. Hacer clic **AHORRAR**.

- Desde su navegador web:
  1. Ir a: https://central.bitdefender.com.
  2. Haga clic en **INICIAR SESIÓN**.
  3. Escriba su dirección de correo electrónico y luego haga clic en **PRÓXIMO**.

4. Hacer clic **¿Has olvidado tu contraseña?**.
5. Hacer clic **PRÓXIMO**.
6. Revise su cuenta de correo electrónico y siga las instrucciones que se le proporcionan para establecer una nueva contraseña para su cuenta Bitdefender.

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 puedo gestionar las sesiones asociadas a mi cuenta de Bitdefender?

En su cuenta de Bitdefender tiene la posibilidad de ver las últimas sesiones inactivas y activas iniciadas en los dispositivos asociados a su cuenta. También puede cerrar sesión de forma remota siguiendo estos pasos:

1. Acceso Centro de Bitdefender.
2. Haga clic en el icono en la parte superior derecha de la pantalla.
3. Haga clic en **Sesiones** en el menú deslizante.
4. En la sección **Sesiones activas**, seleccione la opción **CERRAR SESIÓN** junto al dispositivo en el que desee cerrar la sesión.

3.4.3. Analizando con BitDefender

¿Cómo analizo un archivo o una carpeta?

La manera más fácil de 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 dispositivo.

¿Cómo analizo mi sistema

Para llevar a cabo un análisis completo del sistema:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. Haga clic en el botón **Ejecutar análisis** junto a **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, diríjase a .

¿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 dispositivo.

Para programar un análisis:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. Haga clic en ··· junto al tipo de análisis que desea programar: Análisis del sistema o Quick Scan, en la parte inferior de la interfaz y, a continuación, seleccione **Editar**.
   Como alternativa, puede crear un tipo de análisis que se adapte a sus necesidades haciendo clic en **+Crear análisis** junto a **Administrar análisis**.
4. Personalice el análisis según sus necesidades y, a continuación, haga clic en **Siguiente**.

5. Marque la casilla junto a **Elegir para cuándo programar esta tarea**. Seleccione una de las opciones correspondientes para establecer una programación:
   - Al inicio del sistema
   - A diario
   - Semanalmente
   - Mensual

   Si elige Diario, Mensual o Semanal, arrastre el control deslizante a lo largo de la escala para establecer el período de tiempo deseado en el que debe comenzar el análisis programado.

Si opta por crear un nuevo análisis personalizado, aparecerá la ventana **Tarea de análisis**. En ella puede seleccionar las ubicaciones que desea que se analicen.

¿Cómo creo una tarea de análisis personalizada?

Si desea analizar ubicaciones concretas en su dispositivo 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. En el **ANTIVIRUS** panel, haga clic **Abierto**.
2. Haga clic en **+Crear análisis** junto a **Administrar análisis**.
3. En el campo de nombre de la tarea, escriba un nombre para el análisis, seleccione las ubicaciones que le gustaría analizar y, a continuación, haga clic en **SIGUIENTE**.
4. Configure estas opciones generales:
   - **Analizar únicamente aplicaciones**. Puede configurar Bitdefender para analizar solo las aplicaciones a las que accede.
   - **Prioridad de la tarea de análisis**. Puede elegir el impacto que el proceso de análisis debería tener en el rendimiento de su sistema.
     - Automático: la prioridad del proceso de escaneo dependerá de la actividad del sistema. Para asegurarse de que el proceso de análisis no afecte a la actividad del sistema, Bitdefender

decidirá si el proceso de análisis debe ejecutarse con prioridad alta o baja.

- Alta: la prioridad del proceso de escaneo será alta. Al elegir esta opción, permitirá que otros programas se ejecuten más lentamente y disminuirá el tiempo necesario para que finalice el proceso de escaneo.
- Baja: la prioridad del proceso de escaneo será baja. Al elegir esta opción, permitirá que otros programas se ejecuten más rápido y aumentará el tiempo necesario para que finalice el proceso de escaneo.

- **Acciones posteriores al análisis**. Elija la acción que debe llevar a cabo Bitdefender en caso de que no se encuentren amenazas:
  - Mostrar ventana Resumen
  - Dispositivo de apagado
  - Cerrar ventana de escaneo

5. Si desea configurar detalladamente las opciones de análisis, haga clic en **Mostrar opciones avanzadas**.
   Hacer clic **Próximo**.
6. Si lo desea, puede habilitar la opción **Programar tarea de análisis** y, a continuación, elegir cuándo debe iniciarse el análisis personalizado que ha creado.
   - Al inicio del sistema
   - A diario
   - Mensual
   - Semanalmente

   Si elige Diario, Mensual o Semanal, arrastre el control deslizante a lo largo de la escala para establecer el período de tiempo deseado en el que debe comenzar el análisis programado.
7. Hacer clic **Ahorrar** para guardar los ajustes y cerrar la ventana de configuración.
   Dependiendo de las ubicaciones que se escanearán, el escaneo puede demorar un tiempo. Si se encuentran amenazas durante el proceso de

escaneo, se le pedirá que elija las acciones que se llevarán a cabo en los archivos detectados.

Si lo desea, puede volver a ejecutar análisis personalizados previos haciendo clic en la entrada correspondiente en la lista disponible.

¿Cómo puedo evitar que se analice una carpeta?

Bitdefender permite exceptuar del análisis determinados archivos, carpetas o extensiones de archivo.

Las excepciones son para que las utilicen usuarios con conocimientos avanzados en informática y solo 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 carpetas a la lista de excepciones:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. Haga clic en la pestaña **Ajustes**.
4. Haga clic en **Administrar excepciones**.
5. Hacer clic **+Agregar una excepción**.
6. Introduzca la ruta de la carpeta que desea excluir del análisis en el campo correspondiente.
   Alternativamente, puede navegar a la carpeta haciendo clic en el botón de exploración en el lado derecho de la interfaz, selecciónela y haga clic en **DE ACUERDO**.
7. Encienda el interruptor junto a la función de protección que no debe escanear la carpeta. Hay tres opciones:
   - antivirus
   - Prevención de amenazas en línea

- Defensa contra amenazas avanzadas

8. Hacer clic **Ahorrar** 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 excepciones de Bitdefender:

1. Desactivar la protección antivirus en tiempo real de Bitdefender:
   a. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
   b. En el **ANTIVIRUS** panel, haga clic **Abierto**.
   c. En la ventana **Avanzado**, desactive **Bitdefender Residente**. 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. Muestre los objetos ocultos en Windows. Para averiguar cómo hacerlo, consulte ¿Cómo puedo mostrar los objetos ocultos en Windows? (página 127).
3. Restaurar el archivo desde el área de Cuarentena:
   a. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
   b. En el **ANTIVIRUS** panel, haga clic **Abierto**.
   c. Acceda a la ventana **Ajustes** y haga clic en **Administrar cuarentena**.
   d. Seleccione el archivo y, a continuación, haga clic en **Restaurar**.
4. Añada el archivo a la lista de excepciones. Para averiguar cómo hacerlo, consulte ¿Cómo puedo evitar que se analice una carpeta? (página 114).
5. Active la protección antivirus en tiempo real de Bitdefender.

6. Póngase en contacto con nuestros agentes de soporte técnico para que podamos eliminar la detección de la actualización de información sobre amenazas. Para averiguar cómo hacerlo, consulte Solicitando Ayuda (página 265).

¿Cómo compruebo qué amenazas 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 escaneo directamente desde el asistente de escaneo, una vez que se completa el escaneo, haciendo clic en **MOSTRAR REGISTRO**.

Para comprobar un registro de análisis o cualquier infección detectada en otro momento:

1. Hacer clic **Notificaciones** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **Todo** pestaña, seleccione la notificación sobre el último escaneo. Aquí es donde puede encontrar todos los eventos de análisis de amenazas, incluidas las amenazas detectadas por el análisis en acceso, los análisis iniciados por el usuario y los cambios de estado para los análisis automáticos.
3. En la lista de notificaciones, puede comprobar qué análisis se han realizado recientemente. Haga clic en una notificación para ver detalles al respecto.
4. Para abrir un registro de análisis, haga clic en **Ver log**.

3.4.4. 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 su información de tarjeta de crédito, número de cuenta o cualquier otra

información sensible que pueda introducir al acceder a diferentes sitios online.

Para mantener sus actividades online protegidas y en privado:

1. Hacer clic **Privacidad** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **SEGURIDAD** panel, haga clic **Ajustes**.
3. En el **pago seguro** ventana, haga clic **Lanzar Safepay**.
4. 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 que contiene para asegurarse de que el ladrón no podrá utilizarla.

Para acceder a las características de Antirrobo desde su cuenta:

1. Acceso Centro de Bitdefender.
2. Selecciona el **Mis dispositivos** panel.
3. Haga clic en la tarjeta del dispositivo deseado y, a continuación, seleccione **Antirrobo**.
4. Seleccione la característica que desea usar:
   - **LOCALIZAR** - muestra la ubicación de su dispositivo en Google Maps.
     Mostrar IP - Muestra la última dirección IP del dispositivo seleccionado.
   - **Alerta**: Envía una alerta al dispositivo.
   - **Bloquear**: Bloquea su dispositivo y establece un código PIN numérico 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**: Elimina toda la información de su dispositivo.

> **Importante**
> Después de borrar un dispositivo, todas las características de Antirrobo dejan de funcionar.

¿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 carpetas de su dispositivo usando el menú contextual de Windows. Para ello, basta con seguir estos pasos:

1. Haga clic con el botón derecho en el archivo o carpeta que desea eliminar permanentemente, escoja Bitdefender y seleccione **Destructor de archivos**.
2. Hacer clic **borrar permanentemente**y luego confirme que desea continuar con el proceso.
   Espere a que Bitdefender termine de triturar los archivos.
3. Los resultados son mostrados. Haga clic en **FINALIZAR** para salir del asistente.

¿Cómo puedo proteger mi cámara web frente a los piratas informáticos?

Puede configurar su producto Bitdefender para que permita o deniegue el acceso de las apps instaladas a su cámara web siguiendo estos pasos:

1. Hacer clic **Privacidad** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **PROTECCIÓN DE VIDEO Y AUDIO** panel, haga clic **Ajustes**.
3. Acceda a la ventana de **Protección de cámaras web** y verá la lista con las aplicaciones que han solicitado acceso a su cámara.
4. Señale la aplicación a la que desea permitir o prohibir el acceso y, a continuación, haga clic en el conmutador representado por una cámara de vídeo, situado junto a ella.
   Para ver lo que los otros usuarios de Bitdefender han decidido hacer con la aplicación seleccionada, haga clic en el icono . Se le notificará

cada vez que una de las aplicaciones de la lista resulte bloqueada por los usuarios de Bitdefender.

Para añadir manualmente aplicaciones a esta lista, haga clic en el botón **Añadir aplicación** y seleccione una de las dos opciones.

- Desde la Tienda Windows
- Desde sus aplicaciones

¿Cómo puedo restaurar manualmente los archivos cifrados cuando falla el proceso de restauración?

En caso de que los archivos cifrados no se puedan restaurar automáticamente, puede hacerlo manualmente siguiendo estos pasos:

1. Hacer clic **Notificaciones** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **Todo** seleccione la notificación sobre el último comportamiento de ransomware detectado y, a continuación, haga clic en **Archivos cifrados**.
3. Se muestra la lista con los archivos cifrados.
   Haga clic en **Recuperar archivos** para continuar.
4. En caso de que falle todo o parte del proceso de restauración, debe elegir la ubicación donde se deben guardar los archivos descifrados. Hacer clic **Restaurar ubicación**y luego elija una ubicación en su PC.
5. Aparece una ventana de confirmación.
   Hacer clic **Finalizar** para finalizar el proceso de restauración.

Los archivos con las siguientes extensiones se pueden restaurar en caso de que se cifren:

.3g2; .3gp; .7z; .ai; .aif; .arj; .asp; .aspx; .avi; .bat; .bin; .bmp; .c; .cda; .cgi; .class; .com ; .cpp; .cs; .css; .csv; .dat; .db; .dbf; .deb;.doc; .docx; .gif; .gz; .h264; .h; .flv; .htm; .html;.ico; .jar; .java; .jpeg; .jpg;.js; .jsp; .key; .m4v; .mdb; .mid; .midi; .mkv; .mp3; .mp4; .mov; .mpg; .mpeg; .ods; .odp;.odt; .ogg; .pdf; .pkg; .php; .pl; .png; .pps; .ppt; .pptx; .ps; .psd; .py; .rar; .rm; .rtf; .sav; .sql; .sh; .svg; .swift; .swf; .tar; .tex; .tif; .tiff; .txt; .xlr; .xls; .xlsx; .xml; .wmv; .vb; .vob; .wav; .wks; .wma; .wpl; .wps; .wpd; .wsf; .z; .zip;

3.4.5. Herramientas de optimización

¿Cómo mejoro el rendimiento de mi sistema?

El rendimiento del sistema depende no solo de la configuración del hardware, como la carga de la CPU, el uso de la memoria y el espacio en el disco duro. También está directamente conectado a la configuración de su software ya su gestión de datos.

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

- Optimice el rendimiento de su sistema con un solo clic (página 120)
- Escanea tu sistema periódicamente (página 120)

Optimice el rendimiento de su sistema con un solo clic

La opción OneClick Optimizer le ahorra un tiempo valioso cuando desea una forma rápida de mejorar el rendimiento de su sistema escaneando, detectando y limpiando rápidamente archivos inútiles.

Para iniciar el proceso de OneClick Optimizer:

1. Hacer clic **Utilidades** en el menú de navegación de la Interfaz de Bitdefender.
2. Haga clic en el **Optimizar** botón.
3. Deje que Bitdefender busque archivos que se puedan eliminar y, a continuación, haga clic en el **Optimizar** botón para finalizar el proceso.

Escanea tu sistema periódicamente

La velocidad de su sistema y su comportamiento general también pueden verse afectados por amenazas.

Asegúrese de escanear su sistema periódicamente, al menos una vez a la semana.

Se recomienda utilizar el Análisis del sistema porque analiza todo tipo de amenazas que ponen en peligro la seguridad de su sistema y también analiza los archivos internos.

Para iniciar el análisis del sistema:

1. Hacer clic **Proteccion** en el menú de navegación en el Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. Hacer clic **Ejecutar escaneo** junto a **Exploración del sistema**.
4. Siga los pasos del asistente.

3.4.6. Información de Utilidad

¿Cómo pruebo mi solución de seguridad?

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 solución de seguridad utilizando un archivo seguro desarrollado a tal fin.

Para probar su solución de seguridad:

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 una amenaza).
   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 una amenaza.
   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 Solicitando Ayuda (página 265).

¿Cómo desinstalo Bitdefender?

Si desea eliminar su Bitdefender Total Security :

- En **ventanas 7**:
  1. Hacer clic **Comenzar**, ir a **Panel de control** y haga doble clic **Programas y características**.
  2. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
  3. Haga clic en **ELIMINAR** en la ventana que aparece.
  4. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.

- En **ventanas 8** y **Windows 8.1**:
  1. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control" directamente en la pantalla de inicio) y luego hacer clic en su icono.
  2. Hacer clic **Desinstalar un programa** o **Programas y características**.
  3. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
  4. Hacer clic **ELIMINAR** en la ventana que aparece.
  5. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.

- En **ventanas 10** y **ventanas 11**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el **Sistema** en el área de Configuración, luego seleccione **aplicaciones**.
  3. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
  4. Hacer clic **Desinstalar** de nuevo para confirmar su elección.
  5. Hacer clic **ELIMINAR** en la ventana que aparece.
  6. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.

> **Nota**
> Este procedimiento de reinstalación eliminará permanentemente los ajustes personalizados.

¿Cómo desinstalo Bitdefender VPN?

El procedimiento para eliminar Bitdefender VPN es similar al empleado para desinstalar otros programas de su dispositivo:

- En **ventanas 7**:
  1. Hacer clic **Comenzar**, ir a **Panel de control** y haga doble clic **Programas y características**.
  2. Busque **Bitdefender VPN** y seleccione **Desinstalar**.
     Espere a que el proceso de desinstalación se complete.
- En **ventanas 8** y **Windows 8.1**:
  1. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control" directamente en la pantalla de inicio) y luego hacer clic en su icono.
  2. Hacer clic **Desinstalar** un programa o **Programas y características**.
  3. Encontrar **Bitdefender VPN** y seleccione **Desinstalar**.
     Espere a que se complete el proceso de desinstalación.
- En **ventanas 10** y **ventanas 11**:
  1. Hacer clic **Comenzar**y luego haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
  3. Encontrar **Bitdefender VPN** y seleccione **Desinstalar**.
  4. Hacer clic **Desinstalar** de nuevo para confirmar su elección.
     Espere a que se complete el proceso de desinstalación.

¿Cómo elimino la extensión Bitdefender Anti-tracker?

Dependiendo del navegador que utilice, siga los pasos que se exponen a continuación para desinstalar la extensión Bitdefender Anti-tracker:

- explorador de Internet
  1. Haga clic en  junto a la barra de búsqueda y, a continuación, seleccione Administrar complementos. Se mostrará una lista con las extensiones instaladas.

2. Haga clic en Bitdefender Anti-tracker.
3. Haga clic en **Desactivar** en la parte inferior derecha.

- Google Chrome

1. Haga clic en ⋮ junto a la barra de búsqueda.
2. Seleccione **Más herramientas** y, a continuación, **Extensiones**. Se mostrará una lista con las extensiones instaladas.
3. Haga clic en **Eliminar** en la tarjeta de Bitdefender Anti-tracker.
4. Haga clic en **Eliminar** en la ventana emergente que aparece.

- Mozilla Firefox

1. Hacer clic ≡ junto a la barra de búsqueda.
2. Seleccione **Complementos** y, a continuación, **Extensiones**. Aparece una lista con las extensiones instaladas.
3. Haga clic en ··· y, a continuación, seleccione **Eliminar**.

¿Cómo apago el dispositivo 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 amenazas. Analizar todo el dispositivo 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 su producto para que apague su sistema cuando el análisis haya acabado.

Suponga que ha terminado de trabajar y quiere irse a dormir. Desearía que Bitdefender comprobase todo su sistema en busca de amenazas.

Para apagar el dispositivo cuando finalice el Quick Scan o el Análisis del sistema:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.

3. En la ventana **Análisis**, haga clic en ··· junto a Quick Scan o Análisis del sistema y, a continuación, seleccione **Editar**.
4. Personalice el análisis según sus necesidades y haga clic en **Siguiente**.
5. Marque la casilla junto a **Elegir para cuándo programar esta tarea** y, a continuación, elija cuándo debe comenzar la tarea.
   Si elige Diario, Mensual o Semanal, arrastre el control deslizante a lo largo de la escala para establecer el período de tiempo deseado en el que debe comenzar el análisis programado.
6. Hacer clic **Ahorrar**.

Para apagar el dispositivo al finalizar un análisis personalizado:

1. Haga clic en ··· junto al análisis personalizado que ha creado.
2. Haga clic en **Siguiente** y, a continuación, haga clic otra vez en **Siguiente**.
3. Marque la casilla junto a **Elegir para cuándo programar esta tarea** y, a continuación, elija cuándo debe comenzar la tarea.
4. Hacer clic **Ahorrar**.

Si no se encuentran amenazas, su dispositivo se apagará.

Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas. Para más información, diríjase a Asistente del análisis Antivirus (página 37).

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

Si su dispositivo 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. Hacer clic **Ajustes** en el menú de navegación de la Interfaz de Bitdefender.
2. Selecciona el **Avanzado** pestaña.
3. Active el **Servidor proxy**.
4. Haga clic en **Cambio de proxy**.
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 Microsoft Edge, 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 dirección IP del servidor proxy.
     - **Puerto**: Introduzca el puerto que Bitdefender utiliza para conectar con el servidor proxy.
     - **Nombre de usuario**: Introduzca un nombre de usuario que el proxy reconozca.
     - **Contraseña**: Escriba una contraseña válida para el usuario especificado 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 **ventanas 7**:
  1. Haga clic en **Inicio**.
  2. Localice **Equipo** en el menú **Inicio**.
  3. Haga clic con el botón derecho **Equipo** y seleccione **Propiedades**.
  4. Mire en **Sistema** para comprobar la información de su sistema.
- En **Windows 8**:
  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.
  2. Seleccione **Propiedades** en el menú inferior.
  3. Consulte el área del sistema para ver su tipo de sistema.
- En **ventanas 10** y **ventanas 11**:
  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 cuando se enfrenta a una amenaza y necesita encontrar y eliminar los archivos infectados, que podrían estar ocultos.

Siga estos pasos para ver los elementos ocultos de Windows:

1. Haga clic en {1}Inicio{2} y acceda al {3}Panel de control{4}.
   En {1}Windows 8{2} y {3}Windows 8.1{4}: Desde la pantalla de inicio de Windows, localice el {5}Panel de control{6} (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) y, a continuación, haga clic en su icono.
2. Seleccione {1}Opciones de carpeta{2}.
3. Acceda a la pestaña {1}Ver{2}.
4. Seleccione {1}Mostrar archivo y carpetas ocultos{2}.
5. Desmarcar {1}Ocultar extensiones para tipos de archivo conocidos{2}.

6. Desmarque {1}Ocultar archivos protegidos del sistema operativo{2}.
7. Haga clic en {1}Aplicar{2} y, a continuación, haga clic en {3}Aceptar{4}.

En **ventanas 10** y **ventanas 11**:

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 {1}Mostrar archivos, carpetas y unidades ocultos{2}.
3. Claro **Ocultar las extensiones para tipos de archivo conocidos**.
4. Claro **Ocultar archivos protegidos del sistema operativo**.
5. Hacer clic **Aplicar**, luego haga clic **DE ACUERDO**.

¿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 dispositivo, 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 **ventanas 7**:
  1. Hacer clic **Comenzar**, ir a **Panel de control** y haga doble clic **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 se complete el proceso de desinstalación y luego reinicie su sistema.

- En **ventanas 8** y **Windows 8.1**:
  1. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control" directamente en la pantalla de inicio) y luego hacer clic en su icono.

2. Hacer clic **Desinstalar un programa** o **Programas y características**.
3. Espere unos momentos hasta que se muestre la lista de software instalado.
4. Busque el nombre del programa que desea eliminar y seleccione **Desinstalar**.
5. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.

- En **ventanas 10** y **ventanas 11**:
  1. Hacer clic **Comenzar**y luego haga clic en Configuración.
  2. Haga clic en el **Sistema** en el área de Configuración, luego seleccione **aplicaciones**.
  3. Busque el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  4. Hacer clic **Desinstalar** de nuevo para confirmar su elección.
  5. Espere a que se complete el proceso de desinstalación y 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. Dichos problemas van desde controladores en conflicto hasta amenazas que impiden que Windows se inicie normalmente. En Modo Seguro solo una cuantas aplicaciones trabajan y Windows carga solo los controladores básicos y un mínimo de componentes del sistema operativo. Por esta razón la mayoría de las amenazas están inactivas cuando se usa Windows en modo seguro y se pueden eliminar fácilmente.

Para iniciar Windows en Modo Seguro:

- En **ventanas 7**:
  1. Reinicie su dispositivo.
  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 funciones de red** si desea tener 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**, **Windows 10** y **Windows 11**:
  1. Acceda a la **Configuración del sistema** en Windows pulsando al mismo tiempo las teclas **Windows y 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, haga clic 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, haga clic en **Reiniciar**. Espere a que se apliquen los nuevos ajustes.

3.5. Resolución de Problemas

3.5.1. Resolución de incidencias comunes

Este capítulo presenta algunos problemas que pueden surgir cuando se utilice BitDefender y le ofrece soluciones posibles para estos problemas. La mayoría de estos problemas pueden ser solucionados mediante la configuración adecuada de la configuración del producto.

- Mi sistema parece que se ejecuta lento (página 131)
- El análisis no se inicia (página 133)
- Ya no puedo usar una app (página 135)
- Qué hacer cuando Bitdefender bloquea un sitio web, un dominio, una dirección IP o una aplicación online que son seguros (página 136)
- Cómo actualizo Bitdefender en una conexión de internet lenta (página 141)
- Los servicios de Bitdefender no responden (página 142)
- Error al eliminar Bitdefender (página 147)
- Mi sistema no se inicia tras la instalación de Bitdefender (página 148)

Si no puede encontrar su problema aquí, o si la solución presentada no lo resuelve, puede contactar con el soporte técnico de BitDefender como se representa en el capítulo Solicitando Ayuda (página 265).

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 el único programa de seguridad instalado en el sistema.**
  Aunque Bitdefender busca y elimina los programas de seguridad encontrados durante la instalación, se recomienda eliminar cualquier otra solución de seguridad que pueda usar antes de instalar

Bitdefender. Para más información, diríjase a ¿Cómo desinstalo otras soluciones de seguridad? (página 128).

- **No se cumplen los requisitos del sistema para ejecutar Bitdefender.**
  Si su dispositivo no cumple los requisitos del sistema, se ralentiza, especialmente cuando se ejecutan varias aplicaciones al mismo tiempo. Para más información, diríjase a Requisitos del sistema (página 16).
- **Ha instalado apps que no utiliza.**
  Cualquier dispositivo 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 de su sistema y su comportamiento general también pueden verse afectados por las amenazas. Spyware, malware, troyanos y adware pasan todos factura al rendimiento de su dispositivo. No olvide analizar su sistema regularmente; al menos una vez a la semana. Se recomienda utilizar el análisis del sistema de Bitdefender porque analiza todo los tipos de amenazas que ponen en peligro la seguridad de su sistema.
  Para iniciar el análisis del sistema:

  1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
  2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
  3. En la ventana **Análisis**, haga clic en **Ejecutar análisis** junto a **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, reinstale Bitdefender:
  - En **ventanas 7**:
    1. Hacer clic **Comenzar**, ir a **Panel de control** y haga doble clic **Programas y características**.
    2. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
    3. Hacer clic **REINSTALAR** en la ventana que aparece.
    4. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.
  - En **ventanas 8** y **Windows 8.1**:
    1. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control" directamente en la pantalla de inicio) y luego hacer clic en su icono.
    2. Hacer clic **Desinstalar** un programa o **Programas y características**.
    3. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
    4. Hacer clic **REINSTALAR** en la ventana que aparece.
    5. Espere a que se complete el proceso de reinstalación y luego reinicie su sistema.
  - En **ventanas 10** y **ventanas 11**:
    1. Hacer clic **Comenzar**, luego haga clic **Ajustes**.
    2. Haga clic en el **Sistema** en el área de Configuración, luego seleccione **aplicaciones instaladas**.
    3. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
    4. Hacer clic **Desinstalar** de nuevo para confirmar su elección.
    5. Hacer clic **REINSTALAR** en la ventana que aparece.

6. Espere a que se complete el proceso de reinstalación y luego reinicie su sistema.

> **Nota**
> Al seguir este procedimiento de reinstalación, la configuración personalizada se guarda y está disponible en el nuevo producto instalado. Otros ajustes pueden volver a su configuración predeterminada.

- **Bitdefender no es la única solución de seguridad instalada en su sistema.**
  En este caso:

  1. Eliminar las otras soluciones de seguridad. Para más información, diríjase a ¿Cómo desinstalo otras soluciones de seguridad? (página 128).
  2. Reinstale Bitdefender:
     - En **ventanas 7**:
       a. Hacer clic **Comenzar**, ir a **Panel de control** y haga doble clic **Programas y características**.
       b. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
       c. Hacer clic **REINSTALAR** en la ventana que aparece.
       d. Espere a que se complete el proceso de reinstalación y luego reinicie su sistema.
     - En **ventanas 8** y **Windows 8.1**:
       a. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control" directamente en la pantalla de inicio) y luego hacer clic en su icono.
       b. Hacer clic **Desinstalar** un programa o **Programas y características**.
       c. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
       d. Hacer clic **REINSTALAR** en la ventana que aparece.

e. Espere a que se complete el proceso de reinstalación y luego reinicie su sistema.

- En **ventanas 10** y **ventanas 11**:
  a. Hacer clic **Comenzar**, luego haga clic **Ajustes**.
  b. Haga clic en el **Sistema** en el área de Configuración, luego seleccione **aplicaciones instaladas**.
  c. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
  d. Hacer clic **Desinstalar** de nuevo para confirmar su elección.
  e. Haga clic en **REINSTALAR** en la ventana que aparece
  f. Espere a que se complete el proceso de reinstalación y luego reinicie su sistema.

> **Nota**
> Al seguir este procedimiento de reinstalación, la configuración personalizada se guarda y está disponible en el nuevo producto instalado. Otros ajustes pueden volver a su configuración predeterminada.

Si esta información no le ayuda, puede contactar con el Soporte de BitDefender como se describe en la sección Solicitando Ayuda (página 265).

Ya no puedo usar una app

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 Defensa Contra Amenazas Avanzadas identifica erróneamente ciertas aplicaciones como maliciosas.

Defensa Contra Amenazas Avanzadas es una característica de Bitdefender que monitoriza constantemente las aplicaciones que se ejecutan en su

sistema e informa de las que exhiben comportamientos potencialmente maliciosos. Dado que esta característica se basa en un sistema heurístico, pueden darse casos en los que Defensa Contra Amenazas Avanzadas informe sobre aplicaciones legítimas.

Si se produce esta situación, puede evitar que Advanced Threat Defense monitorice la app correspondiente.

Para añadir el programa a la lista de excepciones:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **DEFENSA AVANZADA CONTRA AMENAZAS** panel, haga clic **Abierto**.
3. En el **Ajustes** ventana, haga clic **Administrar excepciones**.
4. Hacer clic **+Agregar una excepción**.
5. Introduzca en el campo correspondiente la ruta del ejecutable que desea exceptuar del análisis.
   Alternativamente, puede navegar hasta el ejecutable haciendo clic en el botón de exploración en el lado derecho de la interfaz, selecciónelo y haga clic en **DE ACUERDO**.
6. Encienda el interruptor junto a **Defensa contra amenazas avanzadas**.
7. Hacer clic **Ahorrar**.

Si esta información no fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 265).

Qué hacer cuando Bitdefender bloquea un sitio web, un dominio, una dirección IP o una aplicación online que son seguros

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 peligroso un sitio web, un dominio, una dirección IP o una aplicación online que sí son seguros, lo que hará que el análisis de tráfico HTTP de Bitdefender los bloquee erróneamente.

En caso de que la misma página, dominio, dirección IP o aplicación online se bloqueen en repetidas ocasiones, se pueden añadir a las excepciones

para que los motores de Bitdefender no las analicen, lo que garantiza una navegación sin problemas.

Para añadir un sitio web a las **Excepciones**:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **PREVENCIÓN DE AMENAZAS EN LÍNEA** panel, haga clic **Ajustes**.
3. Hacer clic **Administrar excepciones**.
4. Hacer clic **+Agregar una excepción**.
5. Escriba en el campo correspondiente el nombre del sitio web, el nombre del dominio o la dirección IP que desea agregar a las excepciones.
6. Haga clic en el interruptor junto a **Prevención de amenazas en línea**.
7. Hacer clic **Ahorrar** para guardar los cambios y cerrar la ventana.

Solo debe añadir a esta lista sitios web, dominios, direcciones IP y aplicaciones en los que confíe plenamente. Estos se exceptuarán del análisis por parte de los siguientes motores: amenazas, phishing y fraude.

Si esta información no fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 265).

No me puedo conectar 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. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **CORTAFUEGOS** panel, haga clic **Ajustes**.
3. En el **Normas** ventana, haga clic **Agregar regla**.

4. 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 fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 265).

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 de la siguiente manera:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **CORTAFUEGOS** panel, haga clic **Ajustes**.
3. En el **Normas** ventana, haga clic **Añadir regla**.
4. Active la opción **Aplicar esta regla a todas las aplicaciones**.
5. Haga clic en el botón **Opciones Avanzadas**.
6. En el cuadro **Dirección remota personalizada**, escriba la dirección IP del PC o la impresora a la que desea tener acceso sin restricciones.

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 del otro dispositivo puede bloquear el uso compartido de archivos e impresoras con su PC.
  - Si se está utilizando Firewall de Windows, puede configurarse para que permita compartir archivos e impresoras de la siguiente forma:
    - En **ventanas 7**:

1. Haga clic en **Inicio**, acceda al **Panel de control** y seleccione **Sistema y seguridad**.
2. Acceda a **Windows Firewall** y, a continuación, haga clic en **Permitir un programa a través de Firewall de Windows**.
3. Marque la casilla de verificación **Compartir archivos e impresoras**.

- En **ventanas 8** y **Windows 8.1**:
  1. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control" directamente en la pantalla de inicio) y luego hacer clic en su icono.
  2. Haga clic en **Sistema y seguridad**, acceda a **Windows Firewall** y seleccione **Permitir una aplicación a través de Firewall de Windows**.
  3. Marque la casilla de verificación **Compartir archivos e impresoras** y, a continuación, haga clic en **Aceptar**.

- En **ventanas 10** y **ventanas 11**:
  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, a continuación, 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 dispositivos y a los usuarios solamente. Si esta

compartiendo su impresora, compruebe los permisos establecidos para esta impresora para ver si el usuario de otro dispositivo tiene permitido el acceso a la impresora. Si esta intentando conectarse a una impresora compartida, compruebe con el usuario del otro dispositivo si tiene permisos para conectarse a la impresora.

- La impresora conectada a su dispositivo o al otro no se comparte.
- La impresora compartida no está agregada en el dispositivo.

> **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 dispositivo e usuarios solamente. Debería comprobar con el administrador de red si tiene permisos para conectarse con esta impresora.

Si esta información no fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 265).

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. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el panel **CORTAFUEGO**, desactive el conmutador para desactivar la característica.
3. 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 Solicitando Ayuda (página 265).

- Si tras desactivar el cortafuego de Bitdefender la conexión a Internet mejora:

  a. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.

  b. En el **CORTAFUEGOS** panel, haga clic **Ajustes**.

  c. Acceda a la pestaña **Adaptadores de red** y establezca su conexión a Internet en **Hogar/Oficina**.

  d. En la pestaña **Ajustes**, desactive la **Protección del análisis de puertos**.
  En la zona **Modo oculto**, haga clic en **Editar los ajustes de invisibilidad**. Active el modo Oculto para el adaptador de red al que está conectado.

  e. Cierre Bitdefender, reinicie el sistema y compruebe la velocidad de conexión a Internet.

Si esta información no fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 265).

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 la última base de datos de información de amenazas de Bitdefender:

1. Hacer clic **Ajustes** en el menú de navegación de la Interfaz de Bitdefender.
2. Selecciona el **Actualizar** pestaña.
3. Desactive el conmutador de **Actualización silenciosa**.

4. La próxima vez que haya una actualización disponible, se le pedirá que seleccione la actualización que desea descargar. Seleccione solo **Actualización de firmas**.
5. Bitdefender descargará e instalará solo la base de datos de información de amenazas.

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 de 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 dispositivo 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 dispositivo y espere unos momentos a que Bitdefender se inicie. Abra BitDefender para ver si el error continua. Reiniciando el dispositivo 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, diríjase a ¿Cómo desinstalo otras soluciones de seguridad? (página 128).

Si el error persiste y contacte con nuestros representantes de soporte para conseguir ayuda según se describe en la sección Solicitando Ayuda (página 265).

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]

Los mensajes legítimos se marcan como [spam] simplemente porque al filtro antispam de Bitdefender le parece que lo son. Normalmente puede solucionar este problema configurando adecuadamente el filtro antispam.

Bitdefender añade automáticamente los destinatarios de sus mensajes de correo electrónico a una Lista de amigos. Los mensajes de correo electrónico que reciba de los contactos presentes en la Lista de amigos se considerarán legítimos. El filtro antispam no los verifica y, por lo tanto, no se marcan 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 utiliza uno de los clientes de correo en los que se integra Bitdefender, **Indique detección de errores**.

> **Nota**
> Bitdefender se integra en los clientes de correo más utilizados a través de una barra de herramientas antispam fácil de usar. Para obtener una lista completa de los clientes de correo admitidos, consulte Clientes de correo electrónico y protocolos soportados (página 54).

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** de 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. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el panel **ANTISPAM**, haga clic en **Administrar amigos**.
   Aparece una ventana de configuración.
3. 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 e-mail como desee.
4. Hacer clic **DE ACUERDO** para guardar los cambios y cerrar la ventana.

Indicar 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. Abre tu cliente de correo.
2. Vaya a la carpeta de correo no deseado donde se mueven los mensajes de spam.
3. Seleccione el mensaje legítimos incorrecto marcado como [spam] por Bitdefender.
4. Haga clic en el botón **Añadir amigo** de la barra de herramientas antispam de Bitdefender para añadir el remitente a la Lista de amigos.

Puede que tenga que hacer clic en **Aceptar** para confirmar esta acción. Siempre recibirá mensajes de correo electrónico de esta dirección, independientemente de su contenido.

5. Haga clic en el **No spam** en la barra de herramientas antispam de Bitdefender (normalmente ubicado 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 utiliza uno de los clientes de correo que integra Bitdefender, puede **indicar los mensajes de spam no detectados**.

> **Nota**
> Bitdefender se integra en los clientes de correo más utilizados a través de una barra de herramientas antispam fácil de usar. Para obtener una lista completa de los clientes de correo admitidos, consulte Clientes de correo electrónico y protocolos soportados (página 54).

2. **Añadir remitentes a la lista de emisores de spam**. Los mensajes de correo electrónico recibidos de direcciones que se encuentren en la Lista de emisores de spam se marcarán automáticamente como [spam].

Indicar los mensajes de spam no detectados

Si está utilizando un cliente de correo compatible, puede indicar fácilmente qué mensajes de correo electrónico deberían haberse detectado como spam. Hacerlo ayuda a mejorar la eficiencia del filtro antispam. Sigue estos pasos:

1. Abre tu cliente de correo.
2. Vaya a la carpeta Bandeja de entrada.
3. Seleccione los mensajes de spam no detectados.
4. Haga clic en el botón **Es Spam** en la barra de herramientas antispam de Bitdefender (normalmente ubicada en la parte superior

de la ventana del cliente de correo). Se marcan inmediatamente como [spam] y se mueven 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. Abre tu cliente de correo.
2. Vaya a la carpeta de correo no deseado donde se mueven los mensajes de spam.
3. Seleccione los mensajes marcados como [spam] por BitDefender.
4. Haga clic en el botón **Añadir emisor de spam** de 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. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTISPAM** panel, haga clic **Ajustes**.
3. Acceda a la ventana **Gestionar emisores de spam**.
4. Escriba la dirección de correo electrónico del spammer y luego haga clic en **Añadir**. Puede añadir tantas direcciones de e-mail como desee.
5. Hacer clic **DE ACUERDO** 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 **Protección** en el

menú de navegación de la **interfaz de Bitdefender**. Mire en el panel de **Antispam** si la característica está habilitada.

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 únicamente para clientes de correo configurados para recibir mensajes a través del 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 electrónico está configurado para recibir mensajes por un protocolo distinto de POP3 (por ejemplo, IMAP4), el filtro antispam de Bitdefender no comprobará si se trata de 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 analizar 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 esta sección Solicitando Ayuda (página 265).

Error al eliminar Bitdefender

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 **ventanas 7**:

1. Hacer clic **Comenzar**, ir a **Panel de control** y haga doble clic **Programas y características**.
2. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
3. Hacer clic **ELIMINAR** en la ventana que aparece.
4. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.

- En **ventanas 8** y **Windows 8.1**:
  1. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control" directamente en la pantalla de inicio) y luego hacer clic en su icono.
  2. Hacer clic **Desinstalar un programa** o **Programas y características**.
  3. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
  4. Hacer clic **ELIMINAR** en la ventana que aparece.
  5. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.

- En **ventanas 10** y **ventanas 11**:
  1. Hacer clic **Comenzar**y luego haga clic en Configuración.
  2. Haga clic en el **Sistema** en el área de Configuración, luego seleccione **aplicaciones instaladas**.
  3. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
  4. Hacer clic **Desinstalar** de nuevo para confirmar su elección.
  5. Hacer clic **ELIMINAR** en la ventana que aparece.
  6. Espere a que se complete el proceso de desinstalación y 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:

- **Tenía Bitdefender antes y no lo eliminó correctamente.**
  Para resolver esto:

  1. Reinicie su sistema y entre en Modo seguro. Para averiguar cómo hacerlo, consulte ¿Cómo puedo reiniciar en Modo Seguro? (página 129).
  2. Elimine Bitdefender de su sistema:
     - En **ventanas 7**:
       a. Hacer clic **Comenzar**, ir a **Panel de control** y haga doble clic **Programas y características**.
       b. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
       c. Hacer clic **ELIMINAR** en la ventana que aparece.
       d. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.
       e. Reinicie su sistema en modo normal.
     - En **ventanas 8** y **Windows 8.1**:
       a. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control" directamente en la pantalla de inicio) y luego hacer clic en su icono.
       b. Hacer clic **Desinstalar un programa** o **Programas y características**.
       c. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.
       d. Hacer clic **ELIMINAR** en la ventana que aparece.
       e. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.
       f. Reinicie su sistema en modo normal.
     - En **ventanas 10** y **ventanas 11**:
       a. Hacer clic **Comenzar**y luego haga clic en Configuración.

b. Haga clic en el **Sistema** en el área de Configuración, luego seleccione **aplicaciones instaladas**.

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

d. Hacer clic **Desinstalar** de nuevo para confirmar su elección.

e. Hacer clic **ELIMINAR** en la ventana que aparece.

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

g. Reinicie su sistema en modo normal.

3. Reinstale su producto Bitdefender.

- **Antes tenía instalada una solución de seguridad y no fue eliminada correctamente.**
  Para resolver esto:

  1. Reinicie su sistema y entre en modo seguro. Para saber cómo hacerlo, consulte ¿Cómo puedo reiniciar en Modo Seguro? (página 129).
  2. Elimine las otras soluciones de seguridad de su sistema:
     - En **ventanas 7**:

       a. Hacer clic **Comenzar**, ir a **Panel de control** y haga doble clic **Programas y características**.

       b. Encuentre el nombre del programa que desea eliminar y seleccione {1}Desinstalar{2}.

       c. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.

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

       a. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control" directamente en la pantalla de inicio) y luego hacer clic en su icono.

       b. Hacer clic **Desinstalar un programa** o **Programas y características**.

c. Busque el nombre del programa que desea eliminar y seleccione **Eliminar**.

d. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.

- En **ventanas 10** y **ventanas 11**:

a. Hacer clic **Comenzar**y luego haga clic en Configuración.

b. Haga clic en el **Sistema** en el área de Configuración, luego seleccione **aplicaciones instaladas**.

c. Busque el nombre del programa que desea eliminar y seleccione **Desinstalar**.

d. Espere a que se complete el proceso de desinstalación y 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 y entre en modo seguro. Para saber cómo hacerlo, consulte ¿Cómo puedo reiniciar en Modo Seguro? (página 129).
2. Utilice la opción Restaurar sistema de Windows para restaurar el dispositivo 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 Solicitando Ayuda (página 265).

3.5.2. Eliminación de amenazas de su sistema

Las amenazas pueden afectar a su sistema de diversas formas y el enfoque de Bitdefender depende del tipo de ataque de amenazas. Dado que las amenazas modifican su comportamiento con frecuencia, es difícil establecer un patrón para sus comportamientos y sus acciones.

Hay situaciones en las que Bitdefender no puede eliminar automáticamente la infección de amenazas de su sistema. En cada caso, su intervención es requerida.

- Entorno de rescate (página 152)
- ¿Qué hacer cuando Bitdefender encuentra amenazas en su dispositivo? (página 153)
- ¿Cómo limpio una amenaza de un archivo? (página 154)
- ¿Cómo limpio una amenaza de un archivo de correo electrónico? (página 156)
- ¿Qué hacer si sospecho que un archivo es peligroso? (página 157)
- ¿Qué son los archivos protegidos con contraseña del registro de análisis? (página 157)
- ¿Qué son los elementos omitidos en el registro de análisis? (página 158)
- ¿Qué son los archivos sobre-comprimidos en el registro de análisis? (página 158)
- ¿Por qué ha eliminado automáticamente Bitdefender un archivo infectado? (página 158)

Si no puede encontrar su problema aquí, o si las soluciones presentadas no lo resuelven, puede comunicarse con los representantes de soporte técnico de Bitdefender como se presenta en el capítulo Solicitando Ayuda (página 265).

Entorno de rescate

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

El Entorno de rescate de Bitdefender va integrado con Windows RE.

Iniciar el sistema en Entorno de rescate

Solo puede acceder al Entorno de rescate desde su producto Bitdefender de la siguiente manera:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.

2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. Haga clic en **Abrir** junto a **Entorno de rescate**.
4. Haga clic en **REINICIAR** en la ventana que aparece.
   El Entorno de rescate de Bitdefender se cargará en unos instantes.

Analizar su sistema en el Entorno de rescate

Para analizar su sistema en el Entorno de rescate:

1. Acceda al Entorno de rescate, según se describe en Iniciar el sistema en Entorno de rescate (página 152).
2. El proceso de análisis de Bitdefender se inicia automáticamente en cuanto se carga el sistema en el Entorno de rescate.
3. Espere a que se complete el análisis. Si se detecta cualquier tipo de amenaza, siga las instrucciones para eliminarla.
4. Para salir del Entorno de rescate, haga clic en el botón Cerrar de la ventana con los resultados del análisis.

¿Qué hacer cuando Bitdefender encuentra amenazas en su dispositivo?

Puede descubrir que hay una amenaza en su dispositivo de una de estas maneras:

- Ha analizado su dispositivo y Bitdefender ha encontrado elementos infectados en el.
- Una alerta de amenaza le informa de que Bitdefender ha bloqueado una o varias amenazas en su dispositivo.

En tal caso, actualice Bitdefender para asegurarse de contar con la última base de datos de información de amenazas y ejecute un Análisis del sistema para analizarlo.

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

Advertencia

Si sospecha que el archivo forma parte del sistema operativo Windows o que no se trata de un archivo infectado, no siga estos pasos y póngase en contacto cuanto antes con el servicio de Atención al cliente de Bitdefender.

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. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
   b. En el **ANTIVIRUS** panel, haga clic **Abierto**.
   c. En el **Avanzado** ventana, apagar **Escudo de Bitdefender**.
2. Mostrar objetos ocultos en Windows. Para saber cómo hacerlo, consulte ¿Cómo puedo mostrar los objetos ocultos en Windows? (página 127).
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 y entre en modo seguro. Para saber cómo hacerlo, consulte ¿Cómo puedo reiniciar en Modo Seguro? (página 129).
2. Mostrar objetos ocultos en Windows. Para saber cómo hacerlo, consulte ¿Cómo puedo mostrar los objetos ocultos en Windows? (página 127).
3. Busque la ubicación del archivo infectado (consulte el registro de análisis) y elimínelo.
4. Reiniciar su sistema e iniciar en modo normal.

Si esta información no fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 265).

¿Cómo limpio una amenaza de 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 parcial o totalmente cerrados y Bitdefender solo puede detectar la presencia de amenazas en ellos, pero no realizar ninguna otra acción.

Si Bitdefender le notifica que se ha detectado una amenaza en un archivo y no hay ninguna acción disponible, significa que no es posible eliminar la amenaza debido a restricciones en la configuración de permisos del archivo.

Aquí se explica cómo puede limpiar una amenaza almacenada en un archivo:

1. Identifique el archivo comprimido que incluye la amenaza realizando un Análisis del sistema.
2. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
   b. En el **ANTIVIRUS** panel, haga clic **Abierto**.
   c. En el **Avanzado** ventana, apagar **Escudo de Bitdefender**.
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 una amenaza almacenada en un archivo comprimido no es un peligro inmediato para su sistema, ya que esta debe descomprimirse y ejecutarse para poder infectarlo.

Si esta información no fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 265).

¿Cómo limpio una amenaza de un archivo de correo electrónico?

Bitdefender también puede identificar amenazas en bases de datos de correo electrónico y archivos de correo electrónico almacenados en el disco.

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

Aquí se explica cómo puede limpiar una amenaza almacenada en un archivo de correo electrónico:

1. Analice la base de datos de correo electrónico con Bitdefender.
2. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
   b. En el **ANTIVIRUS** panel, haga clic **Abierto**.
   c. En el **Avanzado** ventana, apagar **Escudo de Bitdefender**.
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 en Administración de archivos de datos. Seleccione los archivos de carpetas personales (.pst) que desea compactar y haga clic en Configuración. Haga clic en Compactar ahora.
   - En Microsoft Outlook 2010/2013/2016: 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 ahora.

6. Active la protección antivirus en tiempo real de Bitdefender.

Si esta información no fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 265).

¿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 averiguar cómo hacerlo, consulte .
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 averiguar cómo hacerlo, consulte Solicitando Ayuda (página 265).

¿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 dispositivo 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 ha eliminado automáticamente Bitdefender un archivo infectado?

Si se detecta un archivo infectado, Bitdefender intentará desinfectarlo automáticamente. Si falla la desinfección, el archivo se traslada a la cuarentena para contener la infección.

Para determinados tipos de amenazas, la desinfección no es posible porque el archivo detectado es completamente malicioso. En tales casos, el archivo infectado se elimina 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.

4. ANTIVIRUS PARA MAC

4.1. Qué es Bitdefender Antivirus for Mac

Bitdefender Antivirus for Mac es un potente analizador antivirus que puede detectar y eliminar todo tipo de software malicioso ("amenazas"), entre las que se incluyen:

- ransomware
- adware
- virus
- spyware
- Troyanos
- keyloggers
- gusanos

Esta aplicación detecta y elimina no solo amenazas de Mac, sino también de Windows, con lo que se evita que envíe accidentalmente archivos infectados a su familia, amigos y compañeros de trabajo que usen PC.

4.2. Instalación y desinstalación

Este capítulo incluye los siguientes temas:

- Requisitos del sistema (página 159)
- Instalación de Bitdefender Antivirus for Mac (página 160)
- Desinstalando Bitdefender Antivirus for Mac (página 164)

4.2.1. Requisitos del sistema

Puede instalar Bitdefender Antivirus for Mac en equipos Macintosh con OS X Yosemite (10.10) o versiones más recientes.

Su Mac también debe tener un mínimo de 1 GB de espacio disponible en disco duro.

Se requiere de una conexión a Internet para registrar y actualizar Bitdefender Antivirus for Mac.

Nota
Bitdefender Anti-tracker y Bitdefender VPN solo se pueden instalar en sistemas que ejecuten macOS 10.12 o versiones más recientes.

Cómo averiguar la versión de macOS y la información de hardware de su Mac
Haga clic en el icono de Apple de la esquina superior izquierda de la pantalla y seleccione Acerca de **este Mac**. En la ventana que aparece, puede ver la versión de su sistema operativo y otros datos de utilidad. Haga clic en **Informe del sistema** para obtener información detallada sobre el hardware.

4.2.2. Instalación de Bitdefender Antivirus for Mac

La aplicación de Bitdefender Antivirus for Mac se puede instalar desde su cuenta de Bitdefender de la siguiente manera:

1. Inicie sesión como administrador.
2. Ir a: https://central.bitdefender.com.
3. Inicie sesión en su cuenta de Bitdefender con su dirección de correo electrónico y contraseña.
4. Seleccione el panel **Mis dispositivos** y, a continuación, toque **INSTALAR PROTECCIÓN**.
5. Escoja una de las dos opciones disponibles:
   - **Proteger este dispositivo**
     a. Seleccione esta opción y, a continuación, seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
     b. Guarde el archivo de instalación.
   - **Proteger otros dispositivos**
     a. Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
     b. Toque **ENVIAR ENLACE DE DESCARGA**.
     c. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR CORREO ELECTRÓNICO**.

Tenga en cuenta que el enlace de descarga generado solo es válido durante las próximas 24 horas. Si caducase, debería generar uno nuevo siguiendo los mismos pasos.

d. En el dispositivo en que desee instalar su producto Bitdefender, compruebe la cuenta de correo electrónico que introdujo y luego haga clic en el botón de descarga correspondiente.

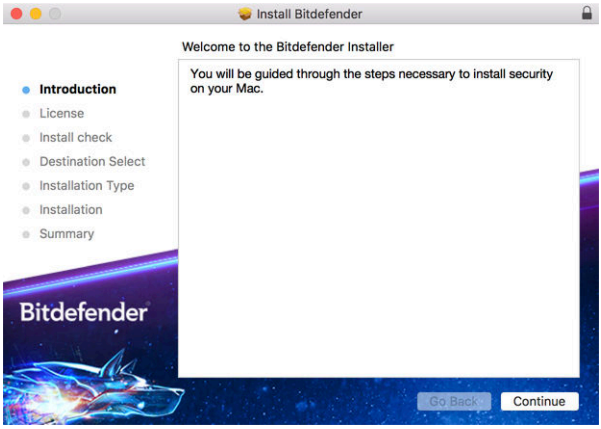
6. Ejecute el producto Bitdefender que ha descargado.
7. Siga los pasos de la instalación.

Proceso de instalación

Para instalar Bitdefender Antivirus for Mac:

1. Haga clic en el archivo descargado. Se iniciará el instalador que le guiará a través del proceso de instalación.
2. Siga el asistente de instalación.

Paso 1 - Ventana de Bienvenida



Haga clic en **Continuar**.

Paso 2: Lea el Acuerdo de Suscripción

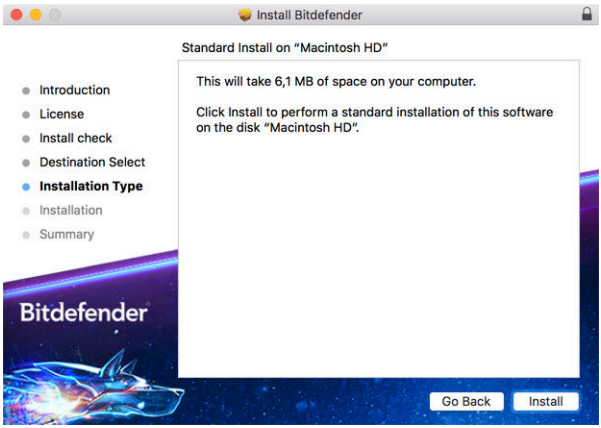
Antes de continuar con la instalación, debe aceptar el Acuerdo de suscripción. Dedique un momento a leerlo, dado que contiene los términos y condiciones bajo los cuales puede usar Bitdefender Antivirus for Mac.

Desde esta ventana también puede seleccionar el idioma en el que desea instalar el producto.

Haga clic en **Continuar** y, luego, haga clic en **Aceptar**.

> **Importante**
> Si no está de acuerdo con estos términos, haga clic en **Continuar** y, luego, haga clic en **No acepto** para cancelar la instalación y salir del instalador.

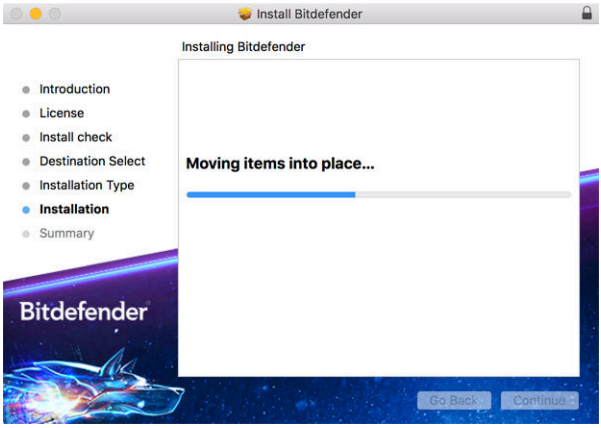
Paso 3 - Iniciar la instalación



Bitdefender Antivirus for Mac se instalará en Macintosh HD/Biblioteca/Bitdefender. La ruta de instalación no se puede cambiar.

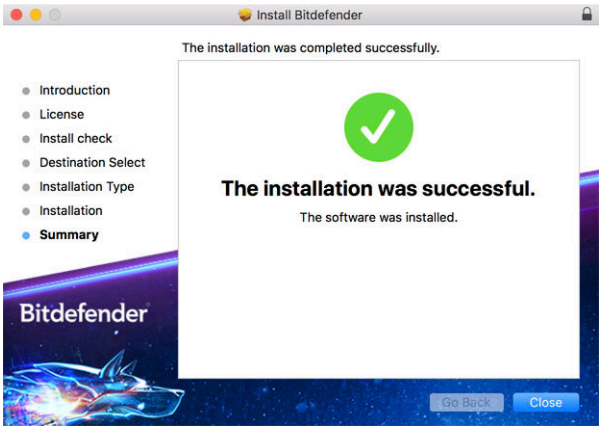
Haga clic en **Instalar** para iniciar la instalación.

Paso 4 - Instalando Bitdefender Antivirus for Mac



Espere hasta que finalice la instalación y, a continuación, haga clic en **Continuar**.

Paso 5 - Finalizar



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

Ha finalizado el proceso de instalación.

Importante

- Si está instalando Bitdefender Antivirus for Mac en macOS High Sierra 10.13.0 o en una versión más reciente, aparecerá la notificación de **Bloqueo de extensión del sistema**. Esta notificación le informa de que las extensiones firmadas por Bitdefender han sido bloqueadas y deben activarse manualmente. Haga clic en Aceptar para continuar. En la ventana que aparece de Bitdefender Antivirus for Mac, haga clic en el enlace **Seguridad y privacidad**. Haga clic en **Permitir** en la parte inferior de la ventana o seleccione Bitdefender SRL en la lista y, luego, haga clic en **Aceptar**.
- Si está instalando Bitdefender Antivirus for Mac en macOS Mojave 10.14 u otra versión más reciente, se mostrará una nueva ventana que le informará de que debe **Conceder acceso total al disco a Bitdefender** y **Permitir la carga de Bitdefender**. Siga las instrucciones que aparecen en la pantalla para configurar adecuadamente el producto.

4.2.3. Desinstalando Bitdefender Antivirus for Mac

Al tratarse de una aplicación compleja, Bitdefender Antivirus for Mac no puede eliminarse de la manera habitual, arrastrando el icono de la aplicación desde la carpeta **Aplicaciones** hasta la papelera.

Para eliminar Bitdefender Antivirus for Mac, siga los pasos que se exponen a continuación:

1. Abra una ventana del **Finder** y luego acceda a la carpeta **Aplicaciones**.
2. Abra la carpeta Bitdefender en **Aplicaciones** y, a continuación, haga doble clic en **BitdefenderUninstaller**.
3. Seleccione la opción de desinstalación que prefiera.

   Nota
   Si intenta eliminar solo la aplicación Bitdefender VPN, seleccione **Desinstalar VPN**.

4. Haga clic en **Desinstalar** y espere a que finalice el proceso.
5. Haga clic en **Cerrar** para finalizar.

   Importante
   Si hay un error, puede contactar con Atención al Cliente de Bitdefender como se describe en Solicitando Ayuda (página 265).

4.3. Iniciando

Este capítulo incluye los siguientes temas:

4.3.1. Abriendo Bitdefender Antivirus for Mac

Hay diferentes maneras de abrir Bitdefender Antivirus for Mac.

- Haga clic en el icono Bitdefender Antivirus for Mac en el Launchpad.
- Haga clic en el icono de la barra de menús y seleccione **Abrir interfaz antivirus**.
- Abra una ventana del Finder, acceda a Aplicaciones y haga doble clic en el icono **Bitdefender Antivirus for Mac**.

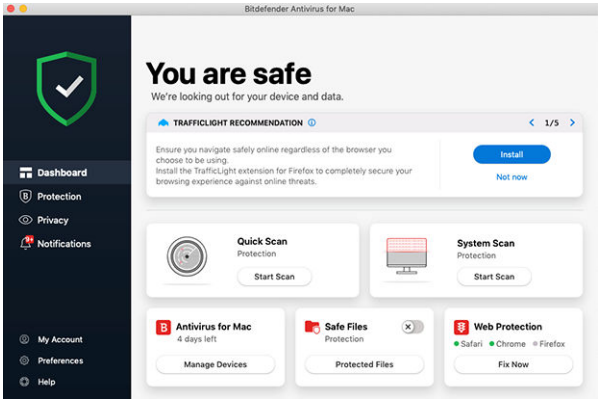
Importante

La primera vez que abra Bitdefender Antivirus for Mac en macOS Mojave 10.14 o en una versión más reciente, aparecerá una recomendación de protección porque necesitamos permisos para analizar todo el sistema en busca de amenazas. Para otorgarnos dichos permisos, debe iniciar sesión como administrador y seguir los pasos que se exponen a continuación:

1. Haga clic en el enlace **Preferencias del sistema**.
2. Haga clic en el icono y, a continuación, introduzca sus credenciales de administrador.
3. Se abre una nueva ventana. Arrastre el archivo **BDLDaemon** a la lista de apps permitidas.

4.3.2. Ventana principal de la app

Bitdefender Antivirus for Mac 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 que conozca la interfaz de Bitdefender, se muestra en la parte superior izquierda un asistente introductorio con información detallada sobre cómo configurar y manejar el producto. Seleccione Seleccione el soporte de ángulo recto para continuar, u **Omitir recorrido** para cerrar el asistente.

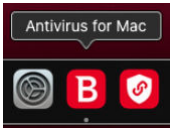
La barra de estado en la parte superior de la ventana le informa sobre el estado de seguridad del sistema mediante mensajes explícitos y colores asociados. Si Bitdefender Antivirus for Mac carece de avisos, la barra de estado es verde. Cuando se detecta un problema de seguridad, la barra de estado se pone roja. Para obtener información detallada sobre cualquier problema y cómo solucionarlo, consulte Reparar Incidencias (página 181).

Para ofrecerle un funcionamiento eficaz y una mayor protección mientras lleva a cabo diferentes actividades, el **Autopilot de Bitdefender** actuará como su asesor de seguridad personal. Dependiendo de la actividad que realice, ya esté trabajando o haciendo pagos por Internet, el Autopilot de Bitdefender le ofrecerá recomendaciones contextuales basadas en el uso y las necesidades de su dispositivo. Esto le ayudará a descubrir y aprovechar las ventajas que le ofrecen las características incluidas en la aplicación de Bitdefender Antivirus for Mac.

Desde el menú de navegación del lado izquierdo, puede acceder a las secciones de Bitdefender para una configuración detallada y tareas administrativas avanzadas (pestañas **Protección** y **Privacidad**), notificaciones, su **cuenta de Bitdefender** y el área de **Preferencias**. Además, puede ponerse en contacto con nosotros (pestaña **Ayuda**) para obtener ayuda en caso de tener alguna pregunta o si sucede algo inesperado.

4.3.3. Icono de app del 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 amenazas. Simplemente arrastre y suelte el archivo o la carpeta en el icono del Dock y el análisis comenzará inmediatamente.



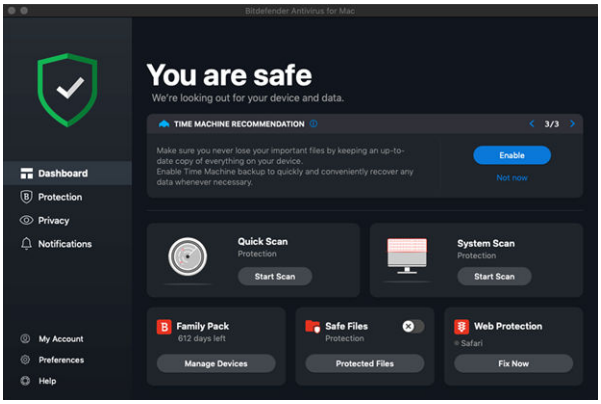
4.3.4. Menú de navegación

En el lado izquierdo de la interfaz de Bitdefender está el menú de navegación, que le permite acceder rápidamente a las características de Bitdefender que necesita para gestionar su producto. Las pestañas disponibles en esta área son las siguientes:

- **Panel de control**. Desde aquí puede solucionar rápidamente los problemas de seguridad, ver recomendaciones según las necesidades de su sistema y sus patrones de uso, realizar acciones rápidas y acceder a su cuenta de Bitdefender para administrar los dispositivos que ha añadido a su suscripción de Bitdefender.
- **Protección**. Desde aquí puede poner en marcha análisis antivirus, añadir archivos a la lista de excepciones, proteger archivos y aplicaciones frente a ataques de ransomware, salvaguardar sus copias de seguridad de Time Machine y configurar su protección mientras navega por Internet.
- **Privacidad**. Desde aquí, puede abrir la aplicación Bitdefender VPN e instalar la extensión Anti-tracker en su navegador.
- **Notificaciones**. Desde aquí puede ver detalles sobre las acciones realizadas en los archivos analizados.
- **Mi Cuenta**. Desde aquí, puede ver la cuenta de Bitdefender y la suscripción que protege a su dispositivo, además de cambiar su cuenta, en caso necesario.
- **Preferencias**. Desde aquí puede configurar los ajustes de Bitdefender.
- **Ayuda**. Desde aquí, siempre que necesite ayuda para resolver cualquier incidencia con su producto de Bitdefender, puede ponerse en contacto con el servicio de soporte técnico. También puede enviarnos sus comentarios para ayudarnos a mejorar el producto.

4.3.5. Modo oscuro

Para proteger sus ojos del deslumbramiento mientras trabaja de noche o en condiciones de escasa iluminación, Bitdefender Antivirus for Mac ofrece el Modo oscuro para Mojave 10.14 y posterior. Se han optimizado los colores de la interfaz para que pueda usar su Mac sin forzar la vista. La interfaz de Bitdefender Antivirus for Mac se adapta según los ajustes de apariencia de su dispositivo.



4.4. Protección contra Software Malicioso

Este capítulo incluye los siguientes temas:

- Mejores Prácticas (página 169)
- Analizando Su Mac (página 170)
- Asistente del Análisis (página 171)
- Cuarentena (página 172)
- Bitdefender Residente (protección en tiempo real) (página 173)
- Excepciones al análisis (página 174)
- Protección Web (página 175)
- Anti-tracker (página 176)
- Safe Files (página 179)
- Protección de Time Machine (página 180)
- Reparar Incidencias (página 181)
- Notificaciones (página 182)
- Actualizaciones (página 183)

4.4.1. Mejores Prácticas

Para mantener su sistema protegido contra las amenazas y evitar la infección accidental de otros sistemas, siga estas recomendaciones:

- Mantenga habilitado **Bitdefender Residente**, para permitir que Bitdefender Antivirus for Mac analice automáticamente los archivos del sistema.
- Mantenga Bitdefender Antivirus for Mac actualizado con la última información de amenazas y actualizaciones de producto.
- Compruebe y repare regularmente las incidencias reportadas por Bitdefender Antivirus for Mac. Para información detallada, diríjase a Reparar Incidencias (página 181).
- 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 área de notificaciones de Bitdefender. Para más información, acceda a Notificaciones (página 182).
- 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 manera más fácil de analizar un archivo, una carpeta o un disco es arrastrarlos y soltarlos en la ventana de Bitdefender Antivirus for Mac o sobre el 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 (página 185).

4.4.2. Analizando Su Mac

Además de la característica **Bitdefender Residente**, que monitoriza regularmente las aplicaciones instaladas en el equipo en busca de síntomas de amenazas e impide que las nuevas amenazas entren en su sistema, puede analizar su Mac o archivos concretos siempre que desee.

La manera más fácil de analizar un archivo, una carpeta o un disco es arrastrarlos y soltarlos en la ventana de Bitdefender Antivirus for Mac o sobre el icono del Dock. Aparecerá el asistente de análisis que le guiará durante este proceso.

También puede iniciar un análisis de la siguiente manera:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Antivirus**.
3. Haga clic en uno de los tres botones de análisis para iniciar el análisis deseado.
   - **Quick Scan:** busca amenazas 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 del sistema:** Realiza una comprobación exhaustiva en busca de amenazas en todo el sistema. Todos los dispositivos montados se analizarán también.

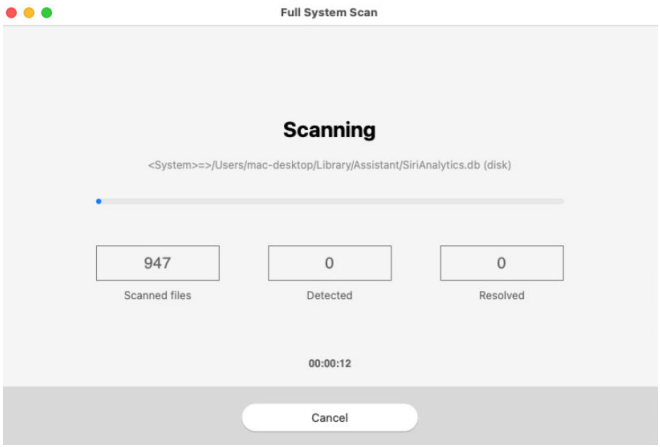
     > **Nota**
     > Dependiendo del tamaño de su disco duro, analizar todo el sistema puede tardar bastante (hasta una hora o incluso más). Para mejorar el rendimiento, se recomienda no ejecutar esta tarea mientras se estén llevando a cabo otras tareas que consuman muchos recursos (como por ejemplo la edición de vídeo).
     >
     > Si lo prefiere, puede escoger no analizar determinados volúmenes montados añadiéndolos a la lista de **Excepciones** en la ventana de Protección.

   - **Análisis personalizado:** le ayuda a comprobar la existencia de amenazas en archivos, carpetas o volúmenes concretos.

También puede iniciar un Quick Scan o un Análisis del sistema desde el panel de control.

4.4.3. Asistente del Análisis

Cuando inicie una análisis, aparecerá el asistente de Análisis de Bitdefender Antivirus for Mac.



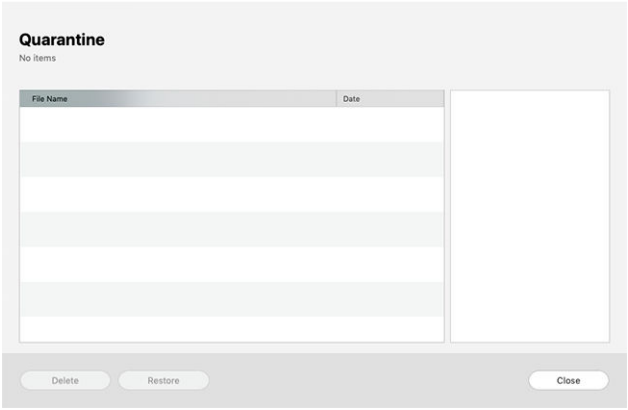
Durante cada análisis se muestra Información en tiempo real acerca de las amenazas detectadas y resueltas.

Espere a que Bitdefender Antivirus for Mac finalice el análisis.

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

4.4.4. Cuarentena

Bitdefender Antivirus for Mac le permite aislar los archivos infectados o sospechosos en una área segura, llamada cuarentena. Cuando una amenaza está aislada en la cuarentena no puede hacer daño alguno, al no poder ejecutarse ni leerse.



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**.

Para ver una lista con todos los elementos añadidos a la cuarentena:

1. Hacer clic **Proteccion** en el menú de navegación de la interfaz de Bitdefender.
2. Haga clic en **Abrir** en el panel de **Cuarentena**.

4.4.5. Bitdefender Residente (protección en tiempo real)

Bitdefender brinda protección en tiempo real contra un amplio abanico de amenazas mediante el análisis de todas las apps instaladas, sus versiones actualizadas y archivos nuevos y modificados.

Para desactivar la protección en tiempo real:

1. Haga clic en **Preferencias** en el menú de navegación de la interfaz de Bitdefender.
2. Desactive **Bitdefender Residente** en la ventana **Protección**.

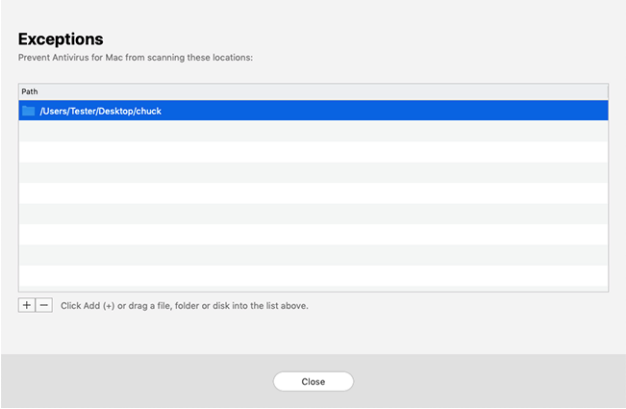
Advertencia

Esto supone un grave problema de seguridad. Le recomendamos que desactive la protección en tiempo real lo menos posible. Si desactiva la protección en tiempo real, no estará protegido contra las amenazas.

4.4.6. Excepciones al 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



La lista de excepciones contiene las rutas que se han exceptuado del análisis.

Para acceder a la lista de excepciones:

1. Hacer clic **Proteccion** en el menú de navegación de la interfaz de Bitdefender.
2. Haga clic en **Abrir** en el panel de **Excepciones**.

Existen dos modos de establecer una excepción de análisis:

- Arrastre y suelte un archivo, carpeta o volumen en la lista de excepciones.
- Hacer clic en el botón etiquetado con el signo más (+), ubicado bajo la lista de excepciones. Luego, escoja el archivo, carpeta o volumen que desee exceptuar del análisis.

Para eliminar una excepción de análisis, selecciónela en la lista y haga clic en el botón etiquetado con el signo menos (-), ubicado bajo la lista de excepciones.

4.4.7. Protección Web

Bitdefender Antivirus for Mac utiliza las extensiones TrafficLight para proteger completamente su navegación por la web. Las extensiones TrafficLight interceptan, procesan y filtran todo el tráfico web para bloquear contenidos maliciosos.

Las extensiones funcionan y se integran con los siguientes navegadores: Mozilla Firefox, Google Chrome y Safari.

Habilitación de extensiones Traffic Light

Para habilitar las extensiones de TrafficLight:

1. Haga clic en **Reparar ahora** en la tarjeta de **Protección web** del panel de control.
2. Se abre la ventana **Protección web**.
   Aparece el navegador detectado que tiene instalado en su sistema. Para instalar la extensión TrafficLight en su navegador, haga clic en **Obtener extensión**.
3. Se le redirige a:
   https://bitdefender.com/solutions/trafficlight.html
4. Seleccione **Descarga gratuita**.
5. Siga los pasos para instalar la extensión TrafficLight correspondiente a su navegador.

Ajustes de administración de extensiones

Hay toda una serie de funciones disponibles para protegerle frente a todo tipo de amenazas que pueda encontrar mientras navega por la Web. Para

acceder a ellos, haga clic en el icono TrafficLight junto a la configuración de su navegador y, a continuación, haga clic en el botón ⚙ **Ajustes**:

- **Ajustes de Bitdefender Traffic Light**
  - Protección web: Evita que acceda a sitios web empleados para ataques de phishing, fraudes y malware.
  - Asesor de búsquedas: Proporciona una advertencia anticipada sobre sitios web peligrosos presentes en sus resultados de búsquedas.
- **Excepciones**
  Si se encuentra en el sitio web que desea añadir a las excepciones, haga clic en **Añadir el sitio web actual a la lista**.
  Si desea añadir otro sitio web, escriba su dirección en el campo correspondiente y, a continuación, haga clic en ⊕.
  No se mostrará ninguna advertencia en caso de que haya amenazas en las páginas exceptuadas. Por eso solo debería añadir a esta lista sitios web en los que confíe plenamente.

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 es una página segura. Puede seguir trabajando.

! Esta página web puede que albergue contenidos peligrosos. Tenga cuidado si desea visitarla.

✖ Debe abandonar la página web de inmediato, ya que contiene malware u otras amenazas.

En Safari, el fondo de los iconos de TrafficLight es negro.

4.4.8. Anti-tracker

Muchos sitios web que visita utilizan rastreadores para recopilar información sobre su comportamiento, ya sea para compartirla con empresas de terceros o para mostrarle anuncios más relevantes para usted. De esta forma, los propietarios de sitios web obtienen dinero para poder brindarle contenidos gratuitos o seguir operando. Además de recopilar información, los rastreadores pueden ralentizar su navegación o desperdiciar su ancho de banda.

Con la extensión Bitdefender Anti-tracker activada en su navegador evita que le rastreen, para mantener la privacidad de sus datos mientras navega y acelerar el tiempo de carga de los sitios web.

La extensión de Bitdefender es compatible con los siguientes navegadores:

- Google Chrome
- Mozilla Firefox
- Safari

Los rastreadores que detectamos se agrupan en las siguientes categorías:

- **Publicidad:** Se utilizan para analizar el tráfico del sitio web, el comportamiento de los usuarios o los patrones de tráfico de los visitantes.
- **Interacción con el cliente:** Se utilizan para medir la interacción del usuario con diferentes sistemas de entrada, como pueden ser un chat o un formulario de soporte.
- **Esencial:** Se utilizan para monitorizar las funciones críticas de la página web.
- **Análisis del sitio:** Se utilizan para recopilar datos sobre el uso de la página web.
- **Redes sociales:** Se utilizan para monitorizar la audiencia, actividad e interacción del usuario con diferentes plataformas de redes sociales.

Activación de Bitdefender Anti-tracker

Para activar la extensión Bitdefender Anti-tracker en su navegador:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Anti-tracker**.
3. Haga clic en **Habilitar extensión** junto al navegador para el cual desee activar la extensión.

Interfaz de Anti-tracker

Cuando se activa la extensión Bitdefender Anti-tracker, aparece el icono junto a la barra de búsqueda en su navegador. Cada vez que visita un sitio web, puede observar un contador en el icono, que hace referencia

a los rastreadores detectados y bloqueados. Para ver más información sobre los rastreadores bloqueados, haga clic en el icono para abrir la interfaz. Además del número de rastreadores bloqueados, puede ver el tiempo necesario para cargar la página y las categorías a las que pertenecen los rastreadores detectados. Para ver la lista de sitios web que le están rastreando, haga clic en la categoría deseada.

Para que Bitdefender deje de bloquear los rastreadores del sitio web que visita actualmente, haga clic en **Pausar la protección en este sitio web**. Este ajuste solo se aplica mientras tenga abierto el sitio web y se revertirá a su estado inicial cuando lo cierre.

Para permitir a los rastreadores de determinada categoría monitorizar su actividad, haga clic en la actividad deseada y luego en el botón correspondiente. Si cambia de parecer, haga clic nuevamente en el mismo botón.

Desactivación de Bitdefender Anti-tracker

Para desactivar la extensión Bitdefender Anti-tracker en su navegador:

1. Abra su navegador Web.
2. Haga clic en el icono junto a la barra de direcciones de su navegador.
3. Haga clic en el icono en la esquina superior derecha.
4. Utilice el conmutador correspondiente para desactivarlo.
   El icono de Bitdefender se vuelve gris.

Permitir el rastreo de un sitio web

Si desea que se le rastree cuando visita determinado sitio web, puede añadir su dirección a las excepciones de la siguiente manera:

1. Abre tu navegador web.
2. Haga clic en el icono junto a la barra de búsqueda.
3. Haga clic en el icono en la esquina superior derecha.
4. Si está en el sitio web que desea agregar a las excepciones, haga clic en **Agregar sitio web actual a la lista**.

Si desea agregar otro sitio web, escriba su dirección en el campo correspondiente y luego haga clic en ⊕.

4.4.9. Safe Files

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.

Gracias a la última tecnología, Bitdefender garantiza la integridad del sistema protegiéndolo contra ataques de ransomware sin afectar a su rendimiento. No obstante, puede que también desee evitar que aplicaciones que no sean de fiar accedan a sus archivos personales, como documentos, fotos o películas. Con Archivos seguros de Bitdefender puede poner a salvo sus archivos personales y configurar qué aplicaciones tienen permiso para realizar cambios en los archivos protegidos y cuáles no.

Para añadir posteriormente archivos al entorno protegido:

1. Hacer clic **Proteccion** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Contra ransomware**.
3. Haga clic en **Archivos protegidos** en el área de Archivos seguros.
4. Hacer clic en el botón etiquetado con el signo más (+), ubicado bajo la lista de archivos protegidos. A continuación, elija el archivo, la carpeta o el volumen que desea proteger en caso de que sufra un ataque de ransomware.

Para evitar que el sistema se ralentice, le recomendamos que añada un máximo de treinta carpetas, o que guarde varios archivos en una sola carpeta.

Las carpetas Imágenes, Documentos, Escritorio y Descargas están protegidas por defecto contra los ataques.

> **Nota**
> Se pueden proteger carpetas personalizadas solo para los usuarios actuales. No se pueden añadir al entorno de protección discos externos, archivos de aplicaciones y del sistema.

Se le informará cada vez que una aplicación desconocida con un comportamiento inusual intente modificar los archivos que ha añadido. Haga clic en **Permitir** o **Bloquear** para añadirlo a la lista de **Aplicaciones administradas**.

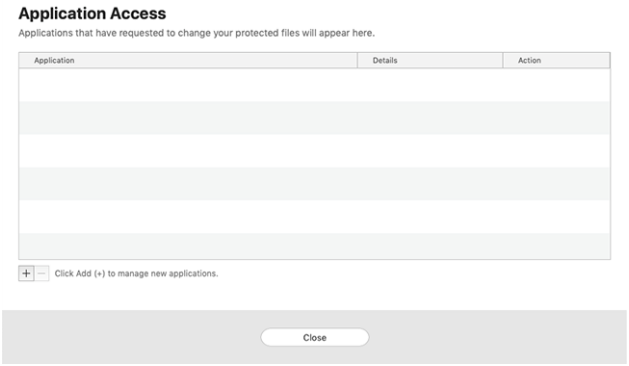
Acceso a las aplicaciones

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 permitirla siguiendo estos pasos:

1. Hacer clic **Proteccion** en el menú de navegación de la interfaz de Bitdefender.
2. Selecciona el **Anti-ransomware** pestaña.
3. Haga clic en **Acceso a aplicaciones** en el área de Archivos seguros.
4. Cambie el estado a Permitir junto a la aplicación bloqueada.

Las aplicaciones fijadas en Permitir también se pueden pasar a estado Bloqueado.

Utilice el método de arrastrar y soltar o haga clic en el signo más (+) para añadir más apps a la lista.



4.4.10. 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.

En caso de que necesite restaurar elementos de una copia de seguridad de Time Machine, consulte la página de soporte técnico de Apple para obtener instrucciones.

Activación y desactivación de la Protección de Time Machine

Para activar o desactivar la Protección de Time Machine:

1. Haga clic en **Protección** en el menú de navegación de la **interfaz de Bitdefender**.
2. Selecciona el **Anti-ransomware** pestaña.
3. Active o desactive el conmutador de **Protección de Time Machine**.

4.4.11. 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.

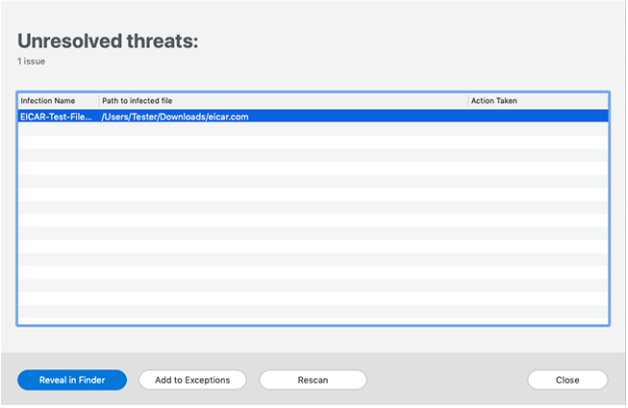
Los problemas detectados incluyen:

- No se ha descargado de nuestros servidores la nueva actualización de la información de amenazas.
- Se han detectado amenazas en su sistema y el producto no puede desinfectarlas automáticamente.
- La protección en tiempo real está desactivada.

Para comprobar y reparar las incidencias detectadas:

1. 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 roja.
2. Compruebe la descripción para más información.

3. Si se detecta un problema, haga clic en el botón correspondiente para adoptar medidas.



La lista de amenazas no resueltas se actualiza tras cada análisis del sistema, independientemente de si el análisis se ha realizado automáticamente en segundo plano o si lo ha iniciado usted.

Puede escoger adoptar las siguientes medidas respecto a las amenazas no solucionadas:

- **Eliminar manualmente.** Lleve a cabo esta acción para eliminar manualmente las infecciones.
- **Añadir a excepciones.** Esta acción no está disponible para amenazas encontradas dentro de archivos comprimidos.

4.4.12. Notificaciones

Bitdefender mantiene un registro detallado de los eventos relacionados con la actividad en su equipo. Siempre que ocurra algo relevante para la seguridad de su sistema o de sus datos, se añadirá un nuevo mensaje al área de Notificaciones de Bitdefender, como si fuera un nuevo mensaje de correo electrónico que apareciese en su bandeja de entrada.

Las notificaciones son una herramienta importante para la supervisión y la administración de su protección de Bitdefender. Por ejemplo, puede comprobar fácilmente si la actualización se realizó correctamente, si se encontraron vulnerabilidades o amenazas 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 **Notificaciones** en el menú de navegación 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 comprobarlos y corregirlos.
- 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.

4.4.13. Actualizaciones

Todos los días se encuentran e identifican nuevas amenazas. Por este motivo es muy importante mantener Bitdefender Antivirus for Mac al día con las últimas actualizaciones de información de amenazas.

La actualización de información de amenazas se realiza al instante, reemplazándose progresivamente los archivos que haya que 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 eliminar las últimas amenazas descubiertas por los laboratorios de Bitdefender.

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. Haga clic en el botón **Acciones** en la barra de menús.
2. Elija **Actualizar la base de datos de información de amenazas**.

Como alternativa, puede solicitar manualmente una actualización pulsando CMD + U.

Puede ver el progreso de actualización y archivos descargados.

Obteniendo Actualizaciones a través de un Servidor Proxy

Bitdefender Antivirus for Mac se puede actualizar solo a través de servidores proxy que no requieran autenticación. No tiene que configurar ningún ajuste de programa.

Si se conecta a Internet a través de un servidor proxy que requiera autenticación, debe pasar regularmente a una conexión directa a Internet para obtener actualizaciones de la información de amenazas.

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.

Hallar información sobre Bitdefender Antivirus for Mac

Para hallar información sobre la versión de Bitdefender Antivirus for Mac que ha instalado, acceda a la ventana **Acerca de**. En la misma ventana, puede acceder al Acuerdo de suscripción, la Política de privacidad y las Licencias de código abierto y leer estos documentos.

Para acceder a la ventana Acerca de:

1. Abrir Bitdefender Antivirus for Mac.
2. En la barra de menús, haga clic en Bitdefender Antivirus for Mac y elija **Acerca de Antivirus for Mac**.

4.5. Preferencias de Configuración

Este capítulo incluye los siguientes temas:

4.5.1. Preferencias de Acceso

Para abrir la ventana de Preferencias de Bitdefender Antivirus for Mac:

- Realice una de estas acciones:
  - Hacer clic **preferencias** en el menú de navegación de la interfaz de Bitdefender.
  - Haga clic en la barra de menú de Bitdefender Antivirus for Mac y escoja **Preferencias**.

4.5.2. 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.

- **Bitdefender Residente.** Bitdefender Residente brinda protección en tiempo real contra un amplio abanico de amenazas mediante el análisis de todas las aplicaciones instaladas, sus versiones actualizadas y archivos nuevos y modificados. Le recomendamos que no desactive Bitdefender Residente pero, en caso necesario, hágalo durante el menor tiempo posible. Si desactiva el Bitdefender Residente, no estará protegido contra las amenazas.
- **Analizar solo archivos nuevos y modificados.** Marque esta casilla de verificación para que Bitdefender Antivirus for Mac analice solo los

archivos que no se han analizado antes o que se han modificado desde su último análisis.

Puede optar por no aplicar este ajuste al análisis personalizado y al de arrastrar y soltar dejando sin marcar la casilla de verificación correspondiente.

- **No analizar el contenido de las copias de seguridad.** Marque 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.

4.5.3. Preferencias avanzadas

Puede elegir una acción general para todas las incidencias y elementos sospechosos hallados durante un proceso de análisis.

Acción para elementos infectados

- **Intentar desinfectar o mover a la cuarentena:** Si se detectan archivos infectados, Bitdefender intentará desinfectarlos (eliminando el código malicioso).
- **No realizar ninguna acción:** No se realizará ninguna acción sobre los archivos detectados.

Acción para elementos sospechosos

- **Mover archivos a la cuarentena:** Si se detectan archivos sospechosos, Bitdefender los moverá a la cuarentena.
- **No tomar ninguna medida** - No se realizará ninguna acción sobre los archivos detectados.

4.5.4. Ofertas especiales

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.

Para activar o desactivar las notificaciones de ofertas especiales:

1. Hacer clic **preferencias** en el menú de navegación de la interfaz de Bitdefender.

2. Seleccione la pestaña **Otros**.
3. Active o desactive el conmutador **Mis ofertas**.

> **Nota**
> La opción **Mis ofertas** está habilitada por defecto.

4.6. 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:
   a. Ir a: https://central.bitdefender.com.
   b. Escriba la información requerida en los campos correspondientes. Los datos que proporcione aquí serán confidenciales.
   c. Antes de seguir adelante, debe aceptar los Términos de uso. Acceda a los Términos de uso y léalos detenidamente, ya que contienen los términos y condiciones bajo los cuales puede usar Bitdefender.
      Además, puede acceder a la Política de privacidad y leerla.
   d. Haga clic en **CREAR CUENTA**.
2. Descargue Bitdefender Antivirus for Mac de la siguiente manera:
   a. Selecciona el **Mis dispositivos** panel y, a continuación, haga clic en **INSTALAR PROTECCIÓN**.
   b. Elija una de las dos opciones disponibles:
      - **Protege este dispositivo**
        i. Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
        ii. Guarde el archivo de instalación.

- **Proteger otros dispositivos**

  i. Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.

  ii. Hacer clic **ENVIAR ENLACE DE DESCARGA**.

  iii. Escriba una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR CORREO ELECTRÓNICO**.
  Tenga en cuenta que el enlace de descarga generado es válido solo durante las próximas 24 horas. Si el enlace caduca, deberá generar uno nuevo siguiendo los mismos pasos.

  iv. En el dispositivo en el que desea instalar su producto Bitdefender, verifique la cuenta de correo electrónico que ingresó y luego haga clic en el botón de descarga correspondiente.

c. Ejecute el producto Bitdefender que ha descargado.

Tengo un código de activación. ¿Cómo puedo añadir su validez a mi suscripción?

Si compró un código de activación de uno de nuestros revendedores o lo recibió como regalo, puede agregar su disponibilidad a su suscripción de Bitdefender.

Para activar una suscripción usando un código de activación, siga estos pasos:

1. Acceso Centro de Bitdefender.
2. Selecciona el **mis Suscripciónes** panel.
3. Haga clic en el **CÓDIGO DE ACTIVACIÓN** botón, luego escriba el código en el campo correspondiente.
4. Hacer clic **ACTIVAR** continuar.

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: Activar la opción **No analizar el contenido de las copias de seguridad** en Preferencias de protección o **Añadir a excepciones** 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, haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.

¿Puedo actualizar Bitdefender Antivirus for Mac a través de un servidor proxy?

Bitdefender Antivirus for Mac puede actualizarse solo a través de servidores proxy que no requieren autenticación. No tiene que configurar ningún ajuste del programa.

Si se conecta a Internet a través de un servidor proxy que requiere autenticación, debe cambiar periódicamente a una conexión directa a Internet para obtener actualizaciones de información sobre amenazas.

¿Cómo desinstalo Bitdefender Antivirus for Mac?

Para eliminar Bitdefender Antivirus for Mac, siga estos pasos:

1. Abra una ventana del **Finder** y luego acceda a la carpeta Aplicaciones.
2. Abra la carpeta Bitdefender y, a continuación, haga doble clic en BitdefenderUninstaller.
3. Hacer clic **Desinstalar** y esperar a que se complete el proceso.
4. Hacer clic **Cerca** para terminar.

> **Importante**
> Si hay un error, puede ponerse en contacto con Atención al cliente de Bitdefender como se describe en Solicitando Ayuda (página 265).

¿Cómo elimino las extensiones TrafficLight de mi navegador?

- Para eliminar las extensiones TrafficLight de Mozilla Firefox, siga los pasos siguientes:
  1. Acceda a **Herramientas** y seleccione **Complementos**.
  2. Seleccione **Extensiones** en la columna izquierda.
  3. Seleccione las extensiones y haga clic en **Eliminar**.
  4. Reinicie el navegador para completar el proceso de eliminación.
- Para eliminar las extensiones TrafficLight de Google Chrome, siga los pasos siguientes:
  1. En la parte superior derecha, haga clic en **Más** ⋮.
  2. Acceda a **Más herramientas** y seleccione **Extensiones**.
  3. Haga clic en el icono **Eliminar** junto a la extensión que desea eliminar.
  4. Haga clic en **Eliminar** para confirmar el proceso de eliminación.
- Para eliminar las extensiones Traffic Light de Safari, siga los pasos siguientes:
  1. Acceda a **Preferencias** o pulse **Comando-Coma (,)**.
  2. Seleccione **Extensiones**.
     Se mostrará una lista con las extensiones instaladas.

3. Seleccione la extensión Bitdefender Traffic Light y, a continuación, haga clic en **Quitar**.
4. Haga clic en **Quitar** para confirmar el proceso de eliminación.

¿Cuándo debo usar Bitdefender VPN?

Debe tener cuidado cuando acceda, descargue o cargue contenidos en internet. Para asegurarse de que se mantiene a salvo mientras navega por la web, le recomendamos que use Bitdefender VPN cuando:

- Desee conectarse a redes inalámbricas públicas.
- Desee acceder a contenidos que normalmente están restringidos en zonas concretas, sin importar si está en su hogar o en el extranjero.
- Desee mantener la privacidad de sus datos personales (nombres de usuario, contraseñas, información de tarjetas de crédito, etc.).
- Desee ocultar su dirección IP.

¿Afecta negativamente Bitdefender VPN a la duración de la batería de mi dispositivo?

Bitdefender VPN está diseñado para proteger sus datos personales, ocultar su dirección IP mientras está conectado a redes inalámbricas inseguras y acceder a contenidos restringidos en ciertos países. Para evitar el consumo innecesario de la batería de su dispositivo, le recomendamos que use VPN solo cuando lo necesite, y que prescinda de él cuando no esté conectado.

¿Por qué parece ir más lento Internet cuando me conecto a través de Bitdefender VPN?

Bitdefender VPN está pensado para brindarle agilidad cuando navega por la web; sin embargo, su conectividad a Internet o la distancia al servidor con el que se conecta pueden producir demoras. De ser así, si no es imprescindible que se conecte desde su ubicación a un servidor lejano (por ejemplo, desde Estados Unidos hasta China), le recomendamos que permita que Bitdefender VPN le conecte automáticamente al servidor más cercano o que encuentre un servidor más próximo a su ubicación actual.

5. SEGURIDAD MÓVIL PARA ANDROID

5.1. ¿Qué es Bitdefender Mobile Security?

Las actividades online, como por ejemplo pagar facturas, hacer reservas hoteleras o adquirir bienes y servicios son cómodas y sencillas. No obstante, como muchas otras actividades que han evolucionado en Internet, conllevan altos riesgos y, si no se actúa de forma segura, los datos personales pueden ser verse comprometidos. ¿Y qué hay más importante que proteger los datos almacenados en sus cuentas online y en su smartphone?

Bitdefender Mobile Security le permite lo siguiente:

- Obtener la mejor protección para su smartphone y tablet Android afectando mínimamente a la duración de la batería.
- Protegerse contra estafas móviles que se basan en enlaces.
- Tener acceso a nuestra VPN protegida para navegar por la web de forma rápida, anónima y segura.
- Localice, bloquee y borre de forma remota su dispositivo Android en caso de pérdida o robo
- Comprobar si su cuenta de correo electrónico se ha visto envuelta en vulneraciones o fugas de datos.

5.2. Iniciando

5.2.1. Requisitos del Dispositivo

Bitdefender Mobile Security funciona en cualquier dispositivo que ejecute Android 5.0 o posterior. Se necesita una conexión a Internet activa para el análisis de amenazas en la nube.

5.2.2. Instalar Bitdefender Mobile Security

- **Desde Bitdefender Central**
  - Para Android
    1. Ir a: https://central.bitdefender.com.

2. Inicie sesión en su cuenta de Bitdefender.
3. Seleccione el panel **Mis dispositivos**.
4. Toque **INSTALAR PROTECCIÓN** y, a continuación, toque **Proteger este dispositivo**.
5. Seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, toque el botón correspondiente.
6. Se le redirigirá a la app **Google Play**. En la pantalla de Google Play, toque la opción de instalación.

- En Windows, iOS y macOS
  1. Ir a: https://central.bitdefender.com.
  2. Inicie sesión en su cuenta de Bitdefender.
  3. Selecciona el **Mis dispositivos** panel.
  4. Pulse **INSTALAR PROTECCIÓN** y, a continuación, pulse **Proteger otros dispositivos**.
  5. Seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, pulse el botón correspondiente.
  6. Pulse **ENVIAR ENLACE DE DESCARGA**.
  7. Introduzca una dirección de correo electrónico en el campo correspondiente y pulse **ENVIAR CORREO ELECTRÓNICO**. Tenga en cuenta que el enlace de descarga generado solo es válido durante las próximas 24 horas. Si caducase, debería generar uno nuevo siguiendo los mismos pasos.
  8. En el dispositivo en que desee instalar Bitdefender, compruebe la cuenta de correo electrónico que introdujo y luego pulse el botón de descarga correspondiente.

- **Desde Google Play**
  Busque Bitdefender Mobile Security para encontrar e instalar la app. Como alternativa, escanee el código QR:

  Antes de llevar a cabo los pasos para la validación, debe aceptar el Acuerdo de suscripción. Por favor, dedique un momento a leer el

Acuerdo de suscripción, dado que contiene los términos y condiciones bajo los cuales puede usar Bitdefender Mobile Security.
Toque **CONTINUAR** para pasar a la siguiente ventana.

5.2.3. Iniciar sesión en su cuenta de Bitdefender

Para usar Bitdefender Mobile Security debe vincular su dispositivo a una cuenta de Bitdefender, Facebook, Google, Apple o Microsoft 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 desde su cuenta de Bitdefender, la app intentará iniciar sesión automáticamente en esa cuenta.

Para vincular su dispositivo a una cuenta de Bitdefender:

1. Escriba su dirección de correo electrónico y contraseña de la cuenta de Bitdefender en los campos correspondientes. Si carece de una cuenta de Bitdefender y desea crear una, seleccione el enlace correspondiente.
2. Toque **INICIAR SESIÓN**.

Para iniciar sesión con una cuenta de Facebook, Google o Microsoft, toque el servicio que desee usar en O iniciar sesión con. Se le redirige a la página de inicio de sesión del servicio seleccionado. Siga las instrucciones para vincular su cuenta a Bitdefender Mobile Security.

> **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.

5.2.4. Configurar la protección

Una vez que inicie sesión en la app, aparecerá la ventana Configurar protección. Para proteger su dispositivo, le recomendamos que siga estos pasos:

- **Estado de la suscripción**. Para que Bitdefender Mobile Security le proteja, debe activar su producto con una suscripción, la cual especifica cuánto tiempo puede utilizar el producto. En cuanto caduque, la app dejará de realizar sus funciones y proteger su dispositivo.

Si posee un código de activación, toque **TENGO UN CÓDIGO** y, luego, toque **ACTIVAR**.
Si ha iniciado sesión con una nueva cuenta de Bitdefender y no tiene un código de activación, puede utilizar el producto sin cargo durante catorce días.

- **Protección web**. Si su dispositivo requiere Accesibilidad para activar la Protección web, toque **ACTIVAR**. Se le redirigirá al menú de Accesibilidad. Toque Bitdefender Mobile Security y, a continuación, active el conmutador correspondiente.
- **Analizador de malware**. Ejecute un análisis puntual del sistema para asegurarse de que su dispositivo está libre de amenazas. Para iniciar el proceso de análisis, toque **ANALIZAR AHORA**.
  Tan pronto como comienza el proceso de análisis, aparece el panel de control. Aquí puede ver el estado de seguridad de su dispositivo.

5.2.5. Panel de Control

Toque el icono Bitdefender Mobile Security en la carpeta de aplicaciones del dispositivo para abrir la interfaz de la app.

El panel de control ofrece información sobre el estado de seguridad de su dispositivo y, mediante Autopilot, le permite mejorar la seguridad de su dispositivo proporcionándole recomendaciones de características.

La tarjeta de estado en la parte superior de la ventana le informa sobre el estado de seguridad del dispositivo mediante mensajes explícitos y ciertos colores. Si Bitdefender Mobile Security no tiene avisos que presentar, la barra de estado es verde. Cuando se detecta un problema de seguridad, la tarjeta de estado se pone roja.

Para ofrecerle un funcionamiento eficaz y una mayor protección mientras lleva a cabo diferentes actividades, el **Autopilot de Bitdefender** actuará como su asesor de seguridad personal. Dependiendo de la actividad que realice, Autopilot de Bitdefender le ofrecerá recomendaciones contextuales basadas en el uso y las necesidades de su dispositivo. Esto le ayudará a descubrir y aprovechar las ventajas que le ofrecen las características incluidas en la app de Bitdefender Mobile Security.

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 y desplazarse fácilmente gracias a la barra de navegación inferior:

Analizador de malware

Le permite iniciar un análisis bajo demanda y habilitar Analizar almacenamiento. Para más información, diríjase a Analizador malware (página 197).

Protección web

Le garantiza una navegación segura por Internet alertándole de posibles páginas web maliciosas. Para más información, diríjase a Protección Web (página 200).

VPN

Cifra la comunicación por Internet y le ayuda a mantener su privacidad sin importar a qué tipo de red se encuentre conectado. Para más información, diríjase a VPN (página 202).

Alerta de fraude

Le mantiene a salvo alertándole de posibles enlaces maliciosos que le lleguen a través de SMS, apps de mensajería y cualquier notificación. Para obtener más información, consulte Alerta de fraude (página 205).

Antirrobo

Le permite activar o desactivar el Antirrobo, así como configurar sus ajustes. Para más información, diríjase a Características Antirrobo (página 207).

Privacidad de cuentas

Comprueba si se ha producido alguna vulneración de datos de sus cuentas en Internet. Para más información, diríjase a Privacidad de la cuenta (página 211).

Bloqueo de apps

Le permite proteger su aplicaciones instaladas mediante el establecimiento de un código de acceso PIN. Para más información, diríjase a Bloqueo de apps (página 213).

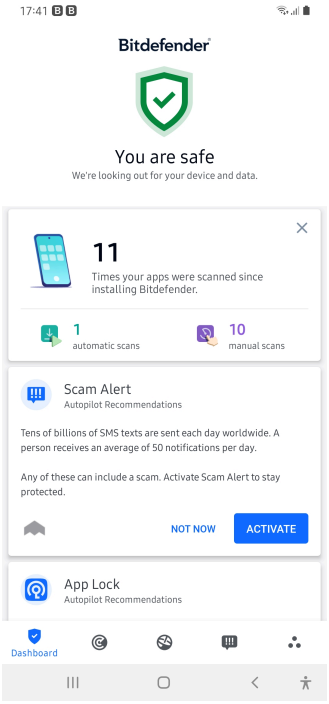
Informes

Mantiene un registro de todas las acciones importantes, cambios de estado y otros mensajes críticos relacionados con la actividad de su

dispositivo. Para obtener más información, consulte Informes (página 217).

WearON

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, diríjase a Localizador (página 218).



5.3. Características y funcionalidades

5.3.1. Analizador malware

Bitdefender protege su dispositivo y sus datos frente a aplicaciones maliciosas utilizando el análisis en la instalación y el análisis bajo demanda.

La interfaz del Analizador de malware proporciona una lista de todos los tipos de amenazas que Bitdefender busca, junto con sus definiciones. Basta con que toque cualquier amenaza para ver su definición.

> **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 al instalar**
  Siempre que instale una aplicación, Bitdefender Mobile Security la analizará automáticamente mediante la tecnología en la nube. Ese mismo proceso de análisis se lleva a cabo cada vez que se actualizan las apps instaladas.
  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 bajo demanda**
  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:

  1. Toque **Analizador de malware** en la barra de navegación inferior.
  2. Toque **INICIAR ANÁLISIS**.

  > **Nota**
  > En Android 6 se requieren permisos adicionales para la característica Analizador de malware. Después de tocar **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 muestra el progreso del análisis, que podrá detener en cualquier momento.

Por defecto, Bitdefender Mobile Security 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.

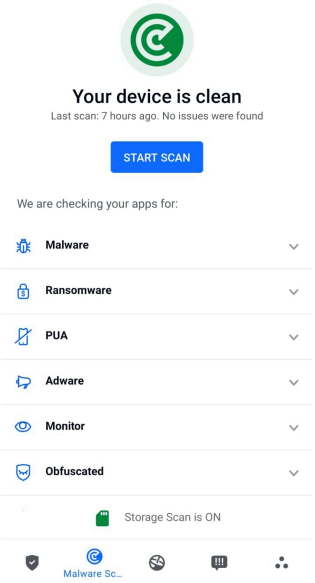
Para deshabilitar el ajuste de Analizar almacenamiento:

1. Toque **Más** en la barra de navegación inferior.
2. Toque **Ajustes**.
3. Desactive el conmutador de **Analizar almacenamiento** en el área del Analizador de malware.

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.

Si la versión de su Android es 7.1 o posterior, puede tener un acceso directo a Malware Scanner para poder ejecutar análisis más rápidamente, sin abrir la interfaz de Bitdefender Mobile Security. Para ello, mantenga pulsado el icono de Bitdefender en su pantalla de inicio o en el cajón de aplicaciones y, a continuación, seleccione el icono .



Detección de anomalías en la aplicación

Bitdefender App AnomalyDetection es una tecnología novedosa integrada en Bitdefender Malware Scanner para proporcionar una capa adicional de protección al monitorear y detectar continuamente cualquier comportamiento malicioso y alertar al usuario si se identifican actividades sospechosas.

La detección de anomalías de aplicaciones de Bitdefender protege a los usuarios incluso cuando, sin saberlo, han instalado una aplicación peligrosa que permanece inactiva durante un período de tiempo o una aplicación aparentemente confiable que interrumpe su funcionalidad y se vuelve maliciosa.

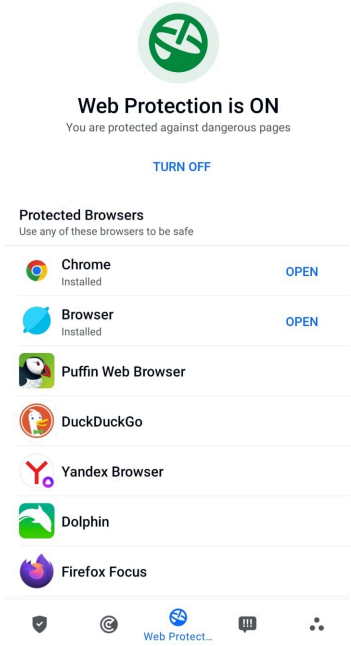
5.3.2. Protección Web

La Protección web comprueba las páginas web de los servicios en la nube de Bitdefender a las que accede con el navegador predeterminado de Android, Google Chrome, Firefox, Firefox Focus, Opera, Opera Mini, Edge, Brave, Samsung Internet, DuckDuckGo, Navegador Yandex, Navegador Huawei y Dolphin.

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.



Protección web de Bitdefender está configurado para decirle que use Bitdefender VPN siempre que accede a un sitio de banca online. Dicha notificación aparece en la barra de estado. Le recomendamos que utilice Bitdefender VPN para conectarse a su cuenta bancaria con el fin de que sus datos permanezcan a salvo de posibles vulneraciones de seguridad.

Para deshabilitar la notificación de Protección web:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Ajustes**.

3. Desactive el conmutador correspondiente en el área de Protección web.

5.3.3. VPN

Con Bitdefender VPN puede mantener la privacidad de sus datos personales cada vez que se conecta a redes inalámbricas inseguras de aeropuertos, centros comerciales, cafeterías u hoteles. De esta forma, se pueden evitar situaciones desafortunadas como el robo de datos personales o que piratas informáticos intenten acceder a la dirección IP de su dispositivo.

La VPN actúa como túnel entre su dispositivo y la red a la que se conecta, para proteger su conexión, cifrar los datos mediante algoritmos de nivel bancario y ocultar su dirección IP dondequiera que esté. Su tráfico se redirige a través de un servidor independiente, lo que hace que su dispositivo sea casi imposible de identificar entre la infinidad de dispositivos que utilizan nuestros servicios. Además, mientras está conectado a Internet a través de VPN, puede acceder a contenidos que normalmente están restringidos en determinadas zonas.

> **Nota**
> Algunos países practican la censura de Internet y, por lo tanto, el uso de las VPN en su territorio está prohibido por la ley. Para evitar responsabilidades legales, puede que aparezca un mensaje de advertencia cuando trate de utilizar la app Bitdefender VPN por primera vez. Al seguir haciendo uso de esa app, confirma que es consciente de las regulaciones nacionales aplicables y de los riesgos a los que podría exponerse.

Hay dos maneras de activar o desactivar Bitdefender VPN:

- Toque **CONECTAR** en la tarjeta de VPN del panel de control.
  Se muestra el estado de Bitdefender VPN.
- Toque **VPN** en la barra de navegación inferior y, a continuación, toque **CONECTAR**.
  Toque **CONECTAR** siempre que desee permanecer protegido mientras se conecte a redes inalámbricas inseguras.
  Toque **DESCONECTAR** cuando desee desactivar la conexión.

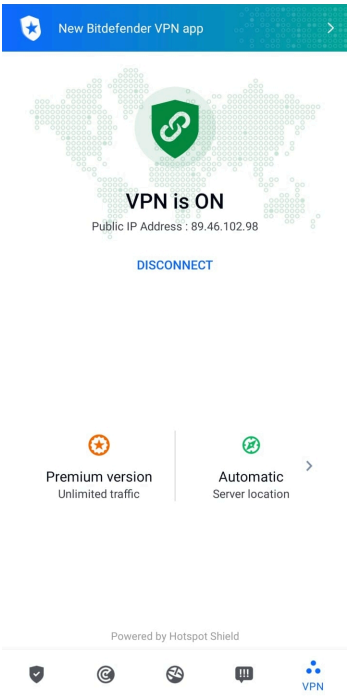
> **Nota**
> Cuando activa VPN por primera vez, se le pide que permita que Bitdefender configure una conexión VPN que monitorice el tráfico de red. Toque **OK** para continuar.

Si la versión de su Android es 7.1 o posterior, puede tener un acceso directo a Bitdefender VPN, sin abrir la interfaz de Bitdefender Mobile Security.

Para ello, mantenga pulsado el icono de Bitdefender en su pantalla de inicio o en el cajón de aplicaciones y, a continuación, seleccione el icono .

Para prolongar la duración de la batería, le recomendamos que desactive la característica VPN cuando no la necesite.

Si posee una suscripción Premium y quiere conectarse a determinado servidor, toque en Ubicación del servidor en la característica de VPN y, a continuación, seleccione el lugar que desee. Para más información sobre las suscripciones a VPN, consulte



Ajustes de VPN

Para una configuración avanzada de su VPN:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Ajustes**.

En el área de VPN puede configurar las siguientes opciones:

- Acceso rápido a VPN: Aparecerá una notificación en la barra de estado de su dispositivo para que pueda activar rápidamente la VPN.
- Advertencia de Wi-Fi abierta: cada vez que se conecte a una red Wi-Fi abierta, se le notificará este hecho en la barra de estado de su dispositivo, para que use la VPN.

Suscripciones

Bitdefender VPN ofrece de forma gratuita una cuota diaria de tráfico de 200 MB por dispositivo para proteger su conexión cada vez que lo necesite y le conecta automáticamente a la ubicación del servidor óptimo.

Para disfrutar de tráfico y acceso ilimitado a contenidos en todo el mundo y elegir la ubicación del servidor que desee, actualice a la versión premium.

Puede actualizar a la versión Bitdefender Premium VPN en cualquier momento tocando **Activar Premium** en la ventana de VPN.

La suscripción a Bitdefender Premium VPN es independiente de la suscripción a Bitdefender Mobile Security, lo que significa que podrá usarla en toda su extensión independientemente del estado de su suscripción de seguridad. En caso de que caduque la suscripción a Bitdefender Premium VPN, pero la de Bitdefender Mobile Security siga activa, se le revertirá al plan gratuito.

Bitdefender VPN es un producto multiplataforma, disponible en los productos Bitdefender compatibles con Windows, macOS, Android y iOS. Una vez que actualice al plan Premium, podrá usar su suscripción en todos los productos, siempre que inicie sesión con la misma cuenta de Bitdefender.

> **Nota**
> Bitdefender VPN también funciona como aplicación independiente en todos los sistemas operativos compatibles: Windows, macOS, iOS y Android.

5.3.4. Alerta de fraude

La característica de Alerta de fraude prioriza las medidas preventivas y aborda situaciones potencialmente peligrosas antes de que puedan convertirse en un problema, incluidas las amenazas de malware. La Alerta de fraude monitoriza en tiempo real todos los mensajes SMS entrantes y notificaciones de Android.

Cuando su teléfono reciba un mensaje con un enlace peligroso, verá una advertencia en la pantalla. Bitdefender le ofrecerá dos opciones. La primera es descartar la información. La segunda opción es **VER DETALLES**. Esto le proporcionará más información sobre el incidente, además de consejos esenciales como los siguientes:

- No abra ni reenvíe el enlace detectado.
- En el caso de los SMS, si es posible, borre el mensaje.
- Bloquee al remitente si no es un contacto de confianza.
- Desinstale la app que envía enlaces peligrosos en sus notificaciones.

> **Nota**
> Debido a limitaciones del sistema operativo Android, Bitdefender no puede eliminar mensajes de texto ni adoptar ninguna medida directa en relación con los mensajes SMS ni con ninguna fuente de notificaciones maliciosas. Si ignora la advertencia de la Alerta de fraude e intenta abrir el enlace peligroso, la característica Protección web de Bitdefender lo detectará automáticamente y evitará que su dispositivo se infecte.

Activación de la Alerta de fraude

Para habilitar la Alerta de fraude, debe otorgar a la app Bitdefender Mobile Security acceso a los mensajes SMS y al sistema de notificaciones:

1. Abra la app Bitdefender Mobile Security instalada en su teléfono o tablet Android.
2. En la pantalla principal de la app de Bitdefender, toque la opción **Alerta de fraude** en la barra de navegación inferior y, a continuación, toque **ACTIVAR**.
3. Toque el botón **PERMITIR**.
4. En la lista de Acceso a notificaciones, pase Bitdefender Security a **ACTIVADO**.
5. Confirme la acción tocando **PERMITIR**.
6. Vuelva a la pantalla de Alerta de fraude y toque **PERMITIR** para que Bitdefender pueda analizar los mensajes SMS entrantes.

Protección de chats en tiempo real

Los mensajes de chat son la manera más cómoda de mantenernos en contacto, pero también facilitan que nos lleguen enlaces peligrosos.

Al activar la característica de Protección de chats, el módulo de Alerta de fraude va más allá de la protección de sus mensajes de texto y notificaciones e incluye también la protección de sus chats contra los ataques basados en enlaces, mediante la detección de enlaces peligrosos en los mensajes de chat que usted envíe o reciba.

Para habilitar la Protección de chats:

1. Abra la aplicación Bitdefender Mobile Security instalada en su teléfono o tableta Android.
2. En la pantalla principal de la app de Bitdefender, toque la opción **Alerta de fraude** en la barra de navegación inferior.
3. Encontrará la función característica de Protección de chat en la parte superior de la pestaña Alerta de fraude. Pase el conmutador correspondiente a la posición **ACTIVADO**.

> **Nota**
> Actualmente, la Protección de chats es compatible con las siguientes aplicaciones:
>
> - WhatsApp
> - Facebook Messenger
> - Telegram
> - Discord

5.3.5. 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.

> **Nota**
> La interfaz de Antirrobo también incluye un enlace a nuestra app de Bitdefender Central en Google Play Store. Puede usar este enlace para descargar la app, en caso de que aún no lo haya hecho.

Bitdefender Mobile Security ofrece las siguientes características de 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 Bitdefender sea capaz de determinarla:

- 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.

Bloqueo remoto

Bloquee la pantalla de su dispositivo y establezca un número PIN para desbloquearla.

Borrado remoto

Borrar todos los datos personales del dispositivo extraviado.

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. Grifo **Más** en la barra de navegación inferior.
2. Toque **Antirrobo**.
3. Toque **ACTIVAR**.

4. Dará comienzo el siguiente procedimiento para ayudarle a activar esta característica:

   > **Nota**
   > En Android 6 se requieren permisos adicionales para la característica Antirrobo.
   >
   > Para activarlo, siga estos pasos:
   >
   > a. Toque **Activar Antirrobo** y, a continuación, toque **ACTIVAR**.
   >
   > b. Dé permiso para que **Antivirus** acceda a la ubicación de este dispositivo

   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 evitar el acceso no autorizado a su dispositivo, debe establecer un código PIN. Cada vez que desee usar su dispositivo, tendrá que introducir primero el PIN. Como alternativa, en los dispositivos que admiten la autenticación mediante huella dactilar, se puede utilizar una confirmación de este tipo en lugar de usar el código PIN configurado.
   El Bloqueo de apps utiliza el mismo código PIN para proteger las aplicaciones que tiene instaladas.

   c. **Activar Hacer foto**
   Si está activada la opción Hacer foto, cada vez que alguien fracase al intentar desbloquear su dispositivo, Bitdefender hará una foto.
   Para ser más exactos, cada vez que se introduce mal tres veces seguidas el código PIN o la confirmación de huella dactilar que estableció para proteger su dispositivo, se hace una foto con la cámara frontal. Dicha foto se guarda junto con el motivo de haberla hecho y la hora, y podrá verla cuando abra Bitdefender Mobile Security y seleccione la característica Antirrobo.
   Como alternativa, puede ver la foto realizada en su cuenta de Bitdefender:

      i. Ir a: https://central.bitdefender.com.

      ii. Inicie sesión en su cuenta.

iii. Selecciona el **Mis dispositivos** panel.

iv. Seleccione su dispositivo Android y, a continuación, la pestaña **Antirrobo**.

v. Toque ⋮ junto a **Consulte sus instantáneas** para ver las últimas fotos que se hicieron.
Solo se guardan las dos últimas fotos.

Una vez activada la función Antirrobo, puede habilitar o deshabilitar los comandos de Control web individualmente desde la ventana de Antirrobo tocando las opciones correspondientes.

Utilización de las características de Antirrobo desde Bitdefender Central

> **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. Selecciona el **Mis dispositivos** panel.
3. En la ventana **MIS DISPOSITIVOS**, seleccione la tarjeta del dispositivo que desee tocando el botón **Ver detalles** correspondiente.
4. Seleccione la pestaña **Antirrobo**.
5. Toque el botón que corresponda a la característica que desea utilizar:
Localizar - muestra la ubicación de su dispositivo en Google Maps.
Mostrar IP - Muestra la última dirección IP del dispositivo seleccionado.
Alerta - escriba un mensaje para mostrarlo en la pantalla de su dispositivo y/o haga que su dispositivo reproduzca una alarma sonora.
Bloquear: Bloquea su dispositivo y establece 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.

Ajustes de Antirrobo

Si desea habilitar o deshabilitar los comandos remotos:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Anti-robo**.
3. Habilitar o deshabilitar las opciones deseadas.

5.3.6. Privacidad de la cuenta

Privacidad de cuentas de Bitdefender detecta si se ha producido alguna vulneración de datos en las cuentas que utiliza para realizar pagos y compras online o para iniciar sesión en diferentes apps o sitios web. Una cuenta puede almacenar datos como contraseñas e información de tarjetas de crédito o de cuentas bancarias y, si no están adecuadamente protegidos, es posible que se produzcan robos de identidad o vulneraciones de la privacidad.

El estado de privacidad de la cuenta se indica justo después de la validación.

Se efectúan nuevas comprobaciones automáticas, configuradas para ejecutarse en segundo plano, pero también se pueden ejecutar análisis manuales a diario.

Se mostrarán notificaciones siempre que se detecten nuevas vulneraciones que afecten a cualquiera de las cuentas de correo electrónico validadas.

Para empezar a poner a salvo su información personal:

1. Grifo **Más** en la barra de navegación inferior.
2. Toque **Privacidad de cuentas**.
3. Toque **PUESTA EN MARCHA**.
4. Aparece la dirección de correo electrónico que utilizara para crear su cuenta de Bitdefender y se añade automáticamente a la lista de cuentas monitorizadas.

5. Para añadir otra cuenta, toque **AÑADIR CUENTA** en la ventana de Privacidad de cuentas y, a continuación, escriba la dirección de correo electrónico.
   Toque **AÑADIR** para continuar.
   Bitdefender tiene que validar esta cuenta antes de mostrar información privada. Por ello, se ha enviado un mensaje con un código de validación a la dirección de correo electrónico proporcionada.
   Compruebe su bandeja de entrada y, a continuación, escriba el código que ha recibido en la zona **Privacidad de la cuenta** de su app. Si no encuentra el mensaje de validación en su bandeja de entrada, compruebe la carpeta de correo no deseado.
   Se muestra el estado de privacidad de la cuenta validada.

En caso de detectarse vulneraciones en cualquiera de sus cuentas, le recomendamos que cambie su contraseña lo antes posible. Para crear una contraseña realmente segura, siga estos consejos:

- Créela de por lo menos ocho caracteres de longitud.
- Utilice una combinación de mayúsculas y minúsculas.
- Incluya al menos un número o un símbolo, como por ejemplo #, @, % o !.

Una vez que haya protegido una cuenta que había sufrido una vulneración de la privacidad, puede confirmar los cambios marcando la vulneración identificada como Solucionada. Para ello:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Privacidad de la cuenta**.
3. Toque la cuenta que acaba de proteger.
4. Toque la vulneración para la que protegió la cuenta.
5. Toque **SOLUCIONADA** para confirmar que la cuenta está protegida.

Cuando todas las vulneraciones detectadas se hayan marcado como **Solucionadas**, la cuenta ya no aparecerá como objeto de vulneraciones, al menos hasta que se vuelva a detectar una nueva vulneración.

Para dejar de recibir notificaciones cada vez que se realicen análisis automáticos:

1. Grifo **Más** en la barra de navegación inferior.

2. Grifo **Ajustes**.
3. Desactive el conmutador correspondiente en el área de Privacidad de la cuenta.

5.3.7. 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.

Se puede recurrir a la autenticación biométrica (como la confirmación mediante huella dactilar o el reconocimiento facial) en lugar de usar el código PIN configurado.

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. Grifo **Más** en la barra de navegación inferior.
2. Toque **Bloqueo de apps**.
3. Grifo **ENCENDER**.
4. Permita el acceso a los datos de uso para Bitdefender Security.
5. Permita **mostrar en otras aplicaciones**.
6. Vuelva a la app, configure el código de acceso y, a continuación, toque **ESTABLECER PIN**.

> **Nota**
> Este paso solo está disponible si no ha configurado previamente el PIN de Antirrobo.

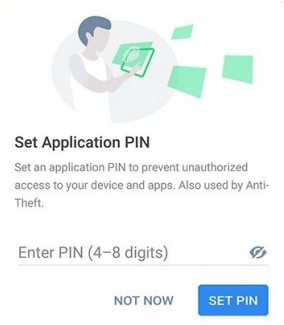
7. Active la opción Hacer foto para identificar a cualquier persona que intente acceder a sus datos privados.

> **Nota**
> En Android 6 se requieren permisos adicionales para la característica Hacer foto. Para activarla, permita que **Antivirus** tome fotos y grabe vídeo.

8. Seleccione las aplicaciones desea proteger.

Si se usa el PIN o la huella dactilar erróneamente cinco veces seguidas, se dejará un tiempo de espera de treinta segundos. Así, se bloqueará cualquier intento de entrada ilegítima en las apps protegidas.

> **Nota**
> El Antirrobo utiliza el mismo código PIN para ayudarle a localizar su dispositivo.



Modo de bloqueo

La primera vez que añada una aplicación al Bloqueo de apps, aparecerá la pantalla del modo de bloqueo de apps. Desde aquí puede elegir cuándo debe el Bloqueo de apps proteger las aplicaciones instaladas en su dispositivo.

Puede escoger una de las siguientes opciones:

- **Requerir el desbloqueo cada vez**: Habrá de utilizar el código PIN o la huella dactilar que ha configurado siempre que acceda a las apps bloqueadas.

- **Mantener desbloqueado hasta que se apague la pantalla**: Podrá acceder libremente a sus aplicaciones hasta que se apague la pantalla.
- **Bloquear después de 30 segundos**: Puede salir y volver a acceder a sus aplicaciones desbloqueadas en un plazo de treinta segundos.

Si desea cambiar el ajuste seleccionado:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Ajustes**.
3. Toque **Requerir el desbloqueo cada vez** en el área del Bloqueo de apps.
4. Escoja la opción deseada.

Opciones de Bloqueo de Apps

Para una configuración avanzada del Bloqueo de apps:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Ajustes**.

En el área del Bloqueo de apps puede configurar las siguientes opciones:

- **Sugerencia de aplicación sensible**: Reciba una notificación de bloqueo cada vez que instale una aplicación sensible.
- **Requerir el desbloqueo cada vez**: Elija una de las opciones disponibles de bloqueo y desbloqueo.
- **Desbloqueo inteligente**: Mantenga las aplicaciones desbloqueadas mientras esté conectado a redes Wi-Fi de confianza.
- **Teclado aleatorio**: Evite la lectura del PIN distribuyendo los números al azar.

Hacer foto

Con Hacer foto de Bitdefender puede poner en una situación comprometida a sus amigos o familiares. De esta manera podrá atajar 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 o la confirmación de huella dactilar que estableció para proteger sus apps, se

toma una foto con la cámara frontal. Dicha foto se guarda junto con el motivo de haberla hecho y la hora, y podrá verla cuando abra Bitdefender Mobile Security 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 para el Bloqueo de apps:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Ajustes**.
3. Active el conmutador correspondiente en el área de Hacer foto.

Las fotos que se tomen cuando se introduzca un PIN incorrecto se mostrarán en la ventana de Bloqueo de apps y se pueden ver a pantalla completa.

Como alternativa, se pueden ver en su cuenta de Bitdefender:

1. Ir a: https://central.bitdefender.com.
2. Iniciar sesión en su cuenta.
3. Seleccione el panel **Mis dispositivos**.
4. Seleccione su dispositivo Android y luego el **Anti-robo** pestaña.
5. Grifo junto a **Revisa tus instantáneas** para ver las últimas fotos que se tomaron.

Solo se guardan las dos fotos más recientes.

Para detener la carga de fotos en su cuenta de Bitdefender:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Ajustes**.
3. Deshabilite **Cargar fotos** en el área de Hacer foto.

Desbloqueo inteligente

Una forma fácil de evitar que el Bloqueo de apps le pida introducir el código PIN o la confirmación de huella dactilar para las apps protegidas cada vez que acceda 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, se deshabilitarán los ajustes del Bloqueo de apps para las aplicaciones protegidas.

Para configurar el Desbloqueo inteligente:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Bloqueo de aplicación**.
3. Toque el botón .
4. Toque el conmutador junto a **Desbloqueo inteligente** si la característica no estuviera habilitada aún.
   Valide con su huella dactilar o su PIN.
   La primera vez que active la característica, deberá habilitar el permiso de ubicación. Toque el botón **PERMITIR** y, a continuación, toque nuevamente **PERMITIR**.
5. Toque **AÑADIR** para establecer la conexión Wi-Fi que utiliza actualmente como red de confianza.

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.

5.3.8. 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. Grifo **Más** en la barra de navegación inferior.
2. Toque **Informes**.

Tiene las siguientes pestañas disponibles en la ventana Informes:

- **INFORMES SEMANALES**: Aquí tiene acceso al estado de seguridad y a las tareas realizadas en la semana actual y anterior. Todos los domingos se genera el informe de la semana en curso. Recibirá una notificación informándole al respecto cuando esté disponible.

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.
Para dejar de recibir notificaciones cada vez que se genera un informe:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Ajustes**.
3. Desactive el conmutador **Notificación de nuevo informe** en el área de Informes.

- **REGISTRO DE ACTIVIDAD**: Aquí puede consultar información detallada sobre la actividad de la app Bitdefender Mobile Security desde que se instaló en su dispositivo Android.
  Para borrar el registro de actividad disponible:

  1. Grifo **Más** en la barra de navegación inferior.
  2. Grifo **Ajustes**.
  3. Toque **Borrar el registro de actividad** y, a continuación, toque **BORRAR**.

5.3.9. 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 tiene activado 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 y activar la característica con el siguiente comando de voz:

Iniciar:<Dónde está mi teléfono>

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, este detectará automáticamente la app en su teléfono y vibrará cuando se aleje mucho y los dispositivos pierdan conectividad Bluetooth.
   Para activar esta característica, abra Bitdefender Mobile Security, 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.

5.3.10. Acerca de

Para hallar información sobre la versión de Bitdefender Mobile Security que tiene instalada, leer el Acuerdo de suscripción y la Política de privacidad, así como ver las licencias de código abierto:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Ajustes**.
3. Toque la opción deseada en el área Acerca de.

5.4. Preguntas frecuentes

¿Por qué necesita Bitdefender Mobile Security 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 cada permiso?

- Acceso a Internet -> Se usa para la comunicación con la nube.
- 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 la nube de Bitdefender.

- Leer y guardar favoritos del navegador -> El módulo de Protección web elimina sitios peligrosos del historial de navegación.
- Leer datos de registro -> Bitdefender Mobile Security detecta signos de amenazas desde los registros de Android.
- Localizar -> Se requiere para la localización remota.
- Cámara -> Necesaria para Hacer foto.
- Almacenamiento -> Se utiliza para permitir que el Analizador de malware compruebe la tarjeta SD.

¿Cómo puedo dejar de enviar información a Bitdefender sobre aplicaciones sospechosas?

Por defecto, Bitdefender Mobile Security envía informes a los servidores de Bitdefender sobre las aplicaciones sospechosas que instala. Esta información es fundamental para mejorar la detección de amenazas y puede ayudarnos a ofrecerle una experiencia de usuario mejor en el futuro. En caso de que desee dejar de enviarnos información sobre aplicaciones sospechosas, haga lo siguiente:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Ajustes**.
3. Desactive **Detección en la nube** en el área del Analizador de malware.

¿Dónde puedo ver detalles sobre la actividad de la aplicación?

Bitdefender Mobile Security mantiene un registro de todas las acciones importantes, cambios de estado y otros mensajes críticos relacionados con su actividad. Para ver la actividad de la aplicación:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Informes**.
   En la ventana INFORMES SEMANALES, puede acceder a los informes que se generan cada semana y en la ventana REGISTRO DE ACTIVIDAD puede ver información sobre la actividad de su aplicación de Bitdefender.

He olvidado el código PIN que establecí para proteger mi aplicación. ¿Qué hago?

1. Acceso Centro de Bitdefender.
2. Selecciona el **Mis dispositivos** panel.
3. Toque la tarjeta del dispositivo deseado y, a continuación, toque ⋮ en la esquina superior derecha de la pantalla.
4. Seleccionar **Ajustes**.
5. Obtenga el código PIN del campo **PIN de aplicación**.

¿Cómo puedo cambiar el código PIN que establecí para el Bloqueo de apps y Antirrobo?

Si desea cambiar el código PIN que estableció para el Bloqueo de apps y Antirrobo:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Ajustes**.
3. Toque **CÓDIGO PIN** de seguridad en el área de Antirrobo.
4. Escriba el código PIN actual.
5. Escriba el nuevo código PIN que desee establecer.

¿Cómo puedo desactivar el Bloqueo de apps?

No existe forma de eliminar el Bloqueo de apps, pero puede desactivarlo fácilmente dejando sin marcar las casillas de verificación junto a las apps seleccionadas después de validar el PIN o la huella dactilar que ha establecido.

¿Cómo puedo configurar otra red inalámbrica para que se considere de confianza?

Primero, debe conectar su dispositivo a la red inalámbrica que desee establecer como red de confianza. A continuación, siga estos pasos:

1. Grifo **Más** en la barra de navegación inferior.
2. Grifo **Bloqueo de aplicación**.
3. Toque en la esquina superior derecha.
4. Toque **AÑADIR** junto a la red que desee establecer como red de confianza.

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

Para dejar de visualizar las fotos tomadas en sus dispositivos:

1. Acceso Centro de Bitdefender.
2. Toque en la parte superior derecha de la pantalla.
3. Toque **Ajustes** en el menú deslizante.
4. Desactive la opción **Mostrar/no mostrar fotos hechas remotamente desde sus dispositivos**.

¿Cómo puedo proteger mis compras online?

Realizar compras online entraña grandes riesgos si se pasan por alto algunos detalles. Para no caer víctima de un fraude, le recomendamos que haga lo siguiente:

- Mantenga actualizada su app de seguridad.
- Realice pagos por Internet solo si cuenta con protección de compras.
- Utilice una VPN cuando se conecte a internet desde lugares públicos o a través de redes inalámbricas que no sean de fiar.
- Preste atención a las contraseñas que ha asignado a sus cuentas de Internet. Deben ser seguras, combinando letras mayúsculas y minúsculas, números y símbolos (@, !, %, #, etc.).
- Asegúrese de enviar la información a través de conexiones seguras. La extensión del sitio web ha de ser HTTPS://, y no HTTP://.

¿Cuándo debo usar Bitdefender VPN?

Debe tener cuidado cuando acceda, descargue o cargue contenidos en internet. Para asegurarse de que se mantiene a salvo mientras navega por la web, le recomendamos que use Bitdefender VPN cuando:

- Desee conectarse a redes inalámbricas públicas.
- Desee acceder a contenidos que normalmente están restringidos en zonas concretas, sin importar si está en su hogar o en el extranjero.
- Desee mantener la privacidad de sus datos personales (nombres de usuario, contraseñas, información de tarjetas de crédito, etc.).
- Desee ocultar su dirección IP.

¿Afecta negativamente Bitdefender VPN a la duración de la batería de mi dispositivo?

Bitdefender VPN está diseñado para proteger sus datos personales, ocultar su dirección IP mientras está conectado a redes inalámbricas

inseguras y acceder a contenidos restringidos en ciertos países. Para evitar el consumo innecesario de la batería de su dispositivo, le recomendamos que use VPN solo cuando lo necesite, y que prescinda de él cuando no esté conectado.

¿Por qué parece ir más lento Internet cuando me conecto a través de Bitdefender VPN?

Bitdefender VPN está pensado para brindarle agilidad cuando navega por la web; sin embargo, su conectividad a Internet o la distancia al servidor con el que se conecta pueden producir demoras. De ser así, si no es imprescindible que se conecte desde su ubicación a un servidor lejano (por ejemplo, desde Estados Unidos hasta China), le recomendamos que permita que Bitdefender VPN le conecte automáticamente al servidor más cercano o que encuentre un servidor más próximo a su ubicación actual.

¿Puedo cambiar la cuenta de Bitdefender vinculada a mi dispositivo?

Sí, puede cambiar fácilmente la cuenta de Bitdefender vinculada a su dispositivo siguiendo los pasos que se indican a continuación:

1. Grifo **Más** en la barra de navegación inferior.
2. Toque su dirección de correo electrónico.
3. Toque **Salir de su cuenta**. Si se ha configurado un código PIN, se le pide que lo escriba.
4. Confirme su elección.
5. Escriba la dirección de correo electrónico y la contraseña de su cuenta en los campos correspondientes y, a continuación, toque **INICIAR SESIÓN**.

¿Cómo afecta Bitdefender Mobile Security al rendimiento y a la batería de mi dispositivo?

Conseguimos un impacto mínimo. La aplicación únicamente se ejecuta cuando es imprescindible – lo que incluye la instalación y cuando se utiliza la interfaz de la aplicación – o cuando quiere comprobar la seguridad. Bitdefender Mobile Security no se ejecuta en segundo plano cuando llama a sus amigos, escribe sus mensajes o juega una partida.

¿Qué es el Administrador de dispositivos?

El Administrador de dispositivos es una característica de Android que da a Bitdefender Mobile Security 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 eliminar completamente sus datos. Si desea desinstalar la app, asegúrese de revocar estos privilegios antes de tratar de desinstalarla desde **Ajustes > Seguridad > Seleccionar administradores de dispositivo**.

Cómo arreglar el error "No Google Token" que aparece cuando se inicia sesión en Bitdefender Mobile Security.

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:

- Acceda en Android a Ajustes > Aplicaciones > Administrar aplicaciones > Bitdefender Mobile Security y toque **Borrar datos**. Luego, intente iniciar sesión nuevamente.
- Asegúrese de que su dispositivo está asociado a una cuenta de Google. Para comprobarlo, acceda a Ajustes > Cuentas y sincronización y mire si existe una cuenta de Google en **Administrar cuentas**. Añada su cuenta si no aparece ninguna, reinicie su dispositivo e intente iniciar sesión en Bitdefender Mobile Security.
- Reinicie su dispositivo y, a continuación, trate de iniciar sesión nuevamente.

¿En qué idiomas está disponible Bitdefender Mobile Security?

Bitdefender Mobile Security está disponible actualmente en los siguientes idiomas:

- Brasileño
- Checo
- Holandés
- Inglés
- Francés
- Alemán
- Griego
- Húngaro
- Italiano

- Japonés
- Coreano
- Polaco
- Portugués
- Rumano
- Ruso
- Español
- Sueco
- Tailandés
- Turco
- Vietnamita

Se añadirán otros idiomas en futuras versiones. Para cambiar el idioma de la interfaz de Bitdefender Mobile Security, vaya a los ajustes **Idioma y texto** de su dispositivo y configure el dispositivo con el idioma que desee utilizar.

6. SEGURIDAD MÓVIL PARA IOS

6.1. Qué es Bitdefender Mobile Security for iOS

Las actividades online, como por ejemplo pagar facturas, hacer reservas hoteleras o adquirir bienes y servicios son cómodas y sencillas. No obstante, como muchas otras actividades que han evolucionado en Internet, conllevan altos riesgos y, si no se actúa de forma segura, los datos personales pueden ser verse comprometidos. ¿Y qué hay más importante que proteger los datos almacenados en sus cuentas online y en su smartphone?

Bitdefender Mobile Security for iOS le permite lo siguiente:

- Ofrece la protección más potente contra amenazas con el menor impacto en la batería
- Proteja sus datos personales: contraseñas, dirección, información financiera y social
- Compruebe fácilmente la seguridad de su teléfono para detectar y corregir las configuraciones erróneas que pueden dejarlo expuesto
- Evite la exposición accidental de sus datos y el uso indebido de todas las apps que tiene instaladas
- Analice su dispositivo para lograr unos ajustes de seguridad y privacidad óptimos
- Obtenga información de uso sobre sus actividades online y el historial de incidentes prevenidos
- Compruebe si sus cuentas online han sido víctimas de vulneraciones o filtraciones de datos
- Cifre el tráfico de Internet con la VPN incluida

Bitdefender Mobile Security for iOS se proporciona de forma gratuita y requiere activarlo con una cuenta de Bitdefender. No obstante, algunas características importantes de Bitdefender, como nuestro módulo 'Protección web', requieren el pago de una suscripción para que nuestros usuarios puedan utilizarlas.

6.2. Iniciando

6.2.1. Requisitos del Dispositivo

Bitdefender Mobile Security for iOS funciona en cualquier dispositivo con iOS 12 o versión superior del sistema operativo y necesita disponer de conexión a Internet para activarse y detectar si se ha producido alguna filtración de datos en sus cuentas online.

6.2.2. Instalación de Bitdefender Mobile Security for iOS

- **Desde Bitdefender Central**
  - Para iOS
    1. Acceda a **Bitdefender Central**.
    2. Seleccione el panel **Mis dispositivos**.
    3. Toque **INSTALAR PROTECCIÓN** y, a continuación, toque **Proteger este dispositivo**.
    4. Seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, toque el botón correspondiente.
    5. Se le redirigirá a la aplicación de **App Store**. En la pantalla de la App Store, toque la opción de instalación.
  - Para Windows, macOS y Android
    1. Acceso Centro de Bitdefender.
    2. Selecciona el **Mis dispositivos** panel.
    3. Pulse **INSTALAR PROTECCIÓN** y, a continuación, pulse **Proteger otros dispositivos**.
    4. Seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, pulse el botón correspondiente.
    5. Pulse **ENVIAR ENLACE DE DESCARGA**.
    6. Introduzca una dirección de correo electrónico en el campo correspondiente y pulse **ENVIAR CORREO ELECTRÓNICO**. Tenga en cuenta que el enlace de descarga generado solo es válido durante las próximas 24 horas. Si caducase, debería generar uno nuevo siguiendo los mismos pasos.

7. En el dispositivo en que desee instalar Bitdefender, compruebe la cuenta de correo electrónico que introdujo y luego pulse el botón de descarga correspondiente.

- **En la App Store**
  Busque Bitdefender Mobile Security for iOS para encontrar e instalar la app.

La primera vez que abra la aplicación, aparecerá una ventana de introducción que le informará sobre las características del producto. Toque Empezar para pasar a la siguiente ventana.

Antes de llevar a cabo los pasos para la validación, debe aceptar el Acuerdo de suscripción. Por favor, dedique un momento a leer el Acuerdo de suscripción, dado que contiene los términos y condiciones bajo los cuales puede usar Bitdefender Mobile Security for iOS.

Toque **Continuar** para pasar a la siguiente ventana.

6.2.3. Iniciar sesión en su cuenta de Bitdefender

Para usar Bitdefender Mobile Security for iOS debe vincular su dispositivo a una cuenta de Bitdefender, Facebook, Google, Apple o Microsoft iniciando sesión en la cuenta desde la app. La primera vez que abra la app se le pedirá que registre una cuenta.

Para vincular su dispositivo a una cuenta de Bitdefender:

1. Introduzca la dirección de correo electrónico de su cuenta de Bitdefender en el campo correspondiente y, a continuación, toque **SIGUIENTE**. Si no tiene una cuenta de Bitdefender y desea crear una, seleccione el enlace correspondiente y luego siga las instrucciones que aparecen en la pantalla hasta activar la cuenta.
   Para iniciar sesión con una cuenta de Facebook, Google, Apple o Microsoft, toque el servicio que desee usar en el área de **O iniciar sesión con**. Se le redirige a la página de inicio de sesión del servicio seleccionado. Siga las instrucciones para vincular su cuenta a Bitdefender Mobile Security for iOS.

> **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.

2. Escriba su contraseña y, a continuación, toque **INICIAR SESIÓN**.

Desde aquí también puede acceder a la Política de privacidad de Bitdefender.

6.2.4. Panel de Control

Toque el icono Bitdefender Mobile Security for iOS en la carpeta de aplicaciones del dispositivo para abrir la interfaz de la aplicación.

La primera vez que accede a la app, se le pide permiso para que Bitdefender le envíe notificaciones. Toque **Permitir<** para estar informado cada vez que Bitdefender tenga que comunicarle algo relevante relacionado con su app. Para administrar las notificaciones de Bitdefender, acceda a Ajustes > Notificaciones > Seguridad móvil.

Para acceder a la sección que necesita, toque el icono correspondiente en la parte inferior de la pantalla.

Protección web

Permanezca a salvo mientras navega por la web y siempre que las aplicaciones menos seguras intenten acceder a dominios que no son de confianza. Para obtener más información, consulte Protección Web (página 233).

VPN

Conserve su privacidad sin importar a qué red se conecte cifrando sus comunicaciones por Internet. Para obtener más información, consulte VPN (página 235).

Privacidad de cuentas

Averigüe si se ha filtrado o no la información de sus cuentas de correo electrónico. Para más información, diríjase a Privacidad de la cuenta (página 238).

Para ver opciones adicionales, toque el icono ••• en su dispositivo mientras esté en la pantalla principal de la aplicación. Aparecerán las siguientes opciones:

- **Restaurar compras**: Desde aquí puede restaurar las suscripciones anteriores que haya adquirido a través de su cuenta de iTunes.
- **Ajustes**: Desde aquí tiene acceso a lo siguiente:
  - **Ajustes de VPN**
    - **Acuerdo**: Puede leer los términos bajo los cuales utiliza el servicio Bitdefender VPN. Si toca **Ya no estoy de acuerdo**, no podrá usar Bitdefender VPN hasta que toque **Estoy de acuerdo**.
    - **Advertencia de red Wi-Fi abierta**: Puede habilitar o no la notificación del producto que aparece cada vez que se conecta a una red Wi-Fi insegura.
      El propósito de esta notificación es ayudarle a mantener la privacidad y seguridad de sus datos mediante el uso de Bitdefender VPN.
  - **Ajustes de Protección web**
    - **Acuerdo**: Puede leer los términos bajo los cuales utiliza el servicio Protección web de Bitdefender. Si toca **Ya no estoy de acuerdo**, no podrá usar Bitdefender VPN hasta que toque **Estoy de acuerdo**.
    - **Notificación de habilitación de la Protección web**: Le notifica que la Protección web se puede habilitar tras finalizar una sesión de VPN.
  - **Informes del producto**.
- **Comentarios**: Desde aquí puede ejecutar el cliente de correo electrónico por defecto para enviarnos sus comentarios acerca de la app.
- **Información de la app**: Desde aquí tiene acceso a la información sobre la versión instalada y el Acuerdo de suscripción, la Política de privacidad y el cumplimiento de las licencias de código abierto.

6.3. Analizar

Bitdefender Mobile Security for iOS le permite analizar su dispositivo en busca de vulnerabilidades de seguridad y amenazas potenciales. Al ejecutar el análisis se comprobará lo siguiente:

- **Versión del sistema operativo:** Comprobación de la versión de iOS para obtener las últimas actualizaciones.
- **Código de acceso/Biometría:** Comprobación del nivel de seguridad de acceso a su dispositivo.
- **Protección web:** Comprobación del estado del módulo de Protección web.
- **Privacidad de cuentas:** Comprobación de la presencia de cuentas monitorizadas incluidas en el módulo de Privacidad de cuentas.
- **Análisis de Wi-Fi:** Comprobación del estado de seguridad de la red a la que se conecta actualmente.

El estado de protección se determina tras ejecutar un análisis manual.

Después de ejecutar el primer análisis, accederá a las recomendaciones de Autopilot de Bitdefender. Se trata de su asesor de seguridad personal, que le proporciona recomendaciones contextuales basadas en el uso y las necesidades de su dispositivo. De esta manera, aprovechará todas las ventajas que su app le ofrece.

> **Nota**
> Cuando acceda a la app por primera vez, se le pedirá que ejecute un análisis.

6.4. Alerta de estafas

La función Alerta de estafa disponible en Bitdefender Mobile Security para iOS protege proactivamente a los usuarios de Apple contra estafas de phishing. Scam Alert para iOS incluye dos capas de protección que monitorean las estafas enviadas a través de mensajes SMS/MMS e invitaciones de calendario:

- **Filtro de mensajes de texto (SMS, MMS)**
  Esta función identifica y filtra mensajes SMS y MMS no deseados.
  Un SMS/MMS (servicio de mensajes cortos/servicio de mensajería multimedia) malicioso se refiere a un tipo de mensaje enviado a dispositivos móviles con intenciones dañinas. Estos mensajes están diseñados para explotar vulnerabilidades, engañar a los destinatarios o causar daños al dispositivo, la información personal o la seguridad del objetivo.

- **Escáner de enlaces de invitación de calendario**
  Esta función detecta calendarios y eventos de spam que contienen enlaces peligrosos. El virus del calendario es un tipo de spam que afecta a la aplicación Calendario de tu iPhone, lo que puede resultar molesto y potencialmente peligroso:
  - Recibe invitaciones de calendario o notificaciones de eventos no deseadas cuando acepta accidentalmente una invitación de calendario falsa enviada a su dirección de correo electrónico por piratas informáticos o spammers.
  - Cuando haces clic en el enlace de la invitación, sin saberlo, te suscribes al calendario del remitente, lo que le permite enviarte más eventos de spam.
  - Los eventos de spam pueden contener enlaces o archivos adjuntos que podrían conducirle a páginas de phishing u otras amenazas cibernéticas si las abre.

6.4.1. Cómo configurar una alerta de estafa

Para habilitar la Alerta de estafa, debe otorgar acceso a la aplicación Bitdefender Mobile Security a las notificaciones del calendario y a los mensajes SMS:

Cómo habilitar el filtrado de SMS:

Para que Bitdefender comience a filtrar mensajes, debe activar manualmente la opción Filtrar remitentes desconocidos en la configuración de la aplicación Mensajes:

1. Abre el **Ajustes** aplicación en tu iPhone o iPad.
2. Desplácese hacia abajo y seleccione **Mensajes** en la lista.
3. Toque en el **Desconocido y spam** sección.
4. Palanca **Filtrar remitentes desconocidos** a la posición de encendido.
5. Seleccionar **Seguridad móvil** en la sección Filtrado de SMS y luego elija **Permitir**.

Bitdefender ahora podrá filtrar mensajes basura en su iPhone/iPad.

> **Nota**
> Debido a las restricciones de iOS, el filtrado de SMS de Bitdefender sólo se puede utilizar para mensajes SMS y MMS que provienen de personas que no tiene guardadas en sus contactos. Esto significa que no filtrará mensajes de personas que ya están en su lista de contactos ni mensajes de iMessage de nadie.

Cómo habilitar el escaneo de calendario:

1. Abre el **Seguridad móvil de Bitdefender** aplicación instalada en su iPhone o iPad.
2. Ve a la **Alerta de estafas** opción en la barra de navegación inferior y presione **Configurar ahora**.
3. Grifo **Continuar** y luego toque **Permitir**.
4. Elegir **DE ACUERDO** para conceder a Bitdefender acceso a su calendario. Se iniciará un análisis del calendario inmediatamente.

6.5. Protección Web

Protección web de Bitdefender le garantiza una navegación segura al alertarle sobre posibles páginas web maliciosas y siempre que las aplicaciones instaladas menos seguras intenten acceder a dominios que no son de confianza.

Cuando una URL apunta a un sitio web conocido de phishing o fraudulento o a contenidos maliciosos como spyware o virus, se bloquea la página web y se muestra una alerta. Lo mismo sucede cuando las aplicaciones instaladas intentan acceder a dominios maliciosos.

> **Importante**
> Si se halla en una región donde la ley restrinja el uso de servicios VPN, la funcionalidad de Protección web no estará disponible.

Para activar la Protección web:

1. Toque el icono en la parte inferior de la pantalla.
2. Toque en **Estoy de acuerdo**.
3. Habilite el conmutador de Protección web.

Nota

Cuando active la Protección web por primera vez, puede que se le pida que permita que Bitdefender establezca configuraciones VPN que monitoricen el tráfico de red. Toque **Permitir** para continuar. Si se ha configurado un método de autenticación (huella dactilar o código PIN) para proteger su smartphone, debe usarlo. Para poder detectar el acceso a dominios que no son de confianza, Protección web trabaja conjuntamente con los servicios de VPN.

Importante

Las características de Protección web y VPN no pueden funcionar simultáneamente. Siempre que una de ellas esté habilitada, la otra (si estuviera activa en ese momento) se inhabilitará.

6.5.1. Alertas de Bitdefender

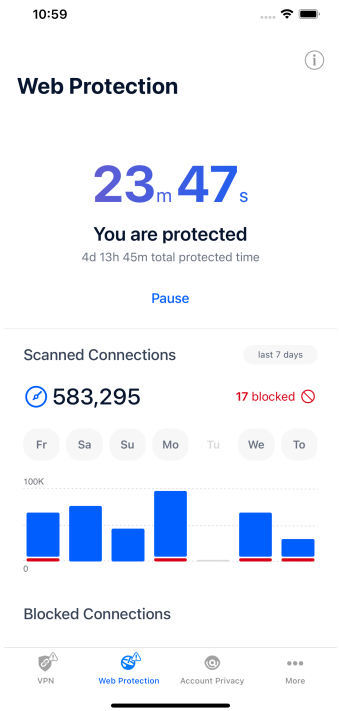
Cada vez que intenta visitar un sitio web clasificado como peligroso, este queda bloqueado. Para informarle de esa circunstancia, Bitdefender utiliza el Centro de notificaciones y su navegador. La página de advertencia contiene información como la URL del sitio web y la amenaza detectada. Tiene que decidir qué hacer a continuación.

Además, en el Centro de notificaciones se le informa siempre que una aplicación menos segura intenta acceder a dominios que no son de confianza. Toque la notificación que se muestra para pasar a la ventana donde puede decidir qué hacer a continuación.

Para ambos casos dispone de las opciones siguientes:

- Abandonar el sitio web tocando **LLÉVAME A UN SITIO SEGURO**.
- Acceder al sitio web, a pesar de la advertencia, tocando la notificación que se muestra y, luego, **Quiero acceder a la página**.

Confirme su elección.



6.6. VPN

Con Bitdefender VPN puede mantener la privacidad de sus datos personales cada vez que se conecta a redes inalámbricas inseguras de aeropuertos, centros comerciales, cafeterías u hoteles. De esta forma, se pueden evitar situaciones desafortunadas como el robo de datos personales o que piratas informáticos intenten acceder a la dirección IP de su dispositivo.

La VPN actúa como túnel entre su dispositivo y la red a la que se conecta para proteger su conexión, cifrar los datos mediante algoritmos de nivel militar y ocultar su dirección IP dondequiera que esté. Su tráfico se redirige a través de un servidor independiente, lo que hace que su dispositivo sea imposible de identificar por su proveedor de Internet entre la infinidad de dispositivos que utilizan nuestros servicios. Además, mientras está conectado a Internet a través de Bitdefender Total Security,

puede acceder a contenidos que normalmente están restringidos en determinadas zonas.

> **Nota**
> Algunos países practican la censura de Internet y, por lo tanto, el uso de las VPN en su territorio está prohibido por la ley. Para evitar responsabilidades legales, puede que aparezca un mensaje de advertencia cuando trate de utilizar la app Bitdefender VPN por primera vez. Al seguir haciendo uso de esa app, confirma que es consciente de las regulaciones nacionales aplicables y de los riesgos a los que podría exponerse.

Para activar Bitdefender VPN:

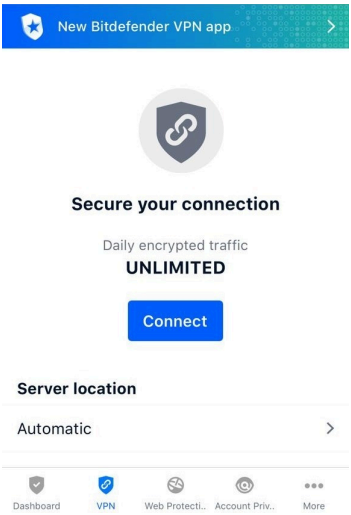
1. Toque en el icono de la parte inferior de la pantalla.
2. Toque **Conectar** siempre que desee permanecer protegido mientras se conecte a redes inalámbricas inseguras.
   Toque **Desconectar** cuando desee desactivar la conexión.

> **Nota**
> Cuando activa VPN por primera vez, se le pide que permita que Bitdefender establezca configuraciones VPN que monitoricen el tráfico de red. Toque **Permitir** para continuar. Si se ha configurado un método de autenticación (huella dactilar o código PIN) para proteger su smartphone, debe usarlo.

El icono VPN aparece en la barra de estado cuando VPN está activo.

Para prolongar la duración de la batería, le recomendamos que desactive VPN cuando no lo necesite.

Si posee una suscripción Premium y quiere conectarse a determinado servidor, toque en Automático en la interfaz de VPN y, a continuación, seleccione el lugar que desee. Para más información sobre las suscripciones a VPN, consulte Suscripciones (página 237).



6.6.1. Suscripciones

Bitdefender VPN ofrece de forma gratuita una cuota diaria de tráfico de 200 MB por dispositivo para proteger su conexión cada vez que lo necesite y le conecta automáticamente a la ubicación del servidor óptimo.

Para disfrutar de tráfico y acceso ilimitado a contenidos en todo el mundo y elegir la ubicación del servidor que desee, actualice a la versión premium.

Puede actualizar a la versión Bitdefender Premium VPN en cualquier momento tocando el botón **Activar Premium VPN** disponible en la ventana de VPN. Hay dos tipos de suscripciones para elegir: anual y mensual.

La suscripción Bitdefender Premium VPN es independiente de la suscripción gratuita a Bitdefender Mobile Security for iOS, lo que significa que podrá usarla en toda su extensión. En caso de que la suscripción Bitdefender Premium VPN caduque, se le revertirá automáticamente al plan gratuito.

Bitdefender VPN es un producto multiplataforma, disponible en los productos Bitdefender compatibles con Windows, macOS, Android y iOS. Una vez que actualice al plan Premium, podrá usar su suscripción en todos los productos, siempre que inicie sesión con la misma cuenta de Bitdefender.

> **Nota**
> Bitdefender VPN también funciona como aplicación independiente en todos los sistemas operativos compatibles: Windows, macOS, iOS y Android.

6.7. Privacidad de la cuenta

Privacidad de la cuenta de Bitdefender detecta si se ha producido alguna filtración de información en las cuentas que utiliza para realizar pagos y compras online, o para iniciar sesión en diferentes apps o sitios web. Una cuenta puede almacenar datos como contraseñas e información de tarjetas de crédito o de cuentas bancarias y, si no están adecuadamente protegidos, es posible que se produzcan robos de identidad o vulneraciones de la privacidad.

El estado de privacidad de la cuenta se indica justo después de la validación.

Para comprobar si se ha filtrado alguna de las cuentas, toque **Buscar filtraciones**.

Para empezar a poner a salvo su información personal:

1. Toque en el icono de la parte inferior de la pantalla.
2. Toque en **Añadir cuenta**.
3. Introduzca su dirección de correo electrónico en el campo correspondiente y, a continuación, toque **Siguiente**.
   Bitdefender tiene que validar esta cuenta antes de mostrar información privada. Por ello, se ha enviado un mensaje con un código de validación a la dirección de correo electrónico proporcionada.
4. Compruebe su bandeja de entrada y, a continuación, escriba el código que ha recibido en la zona **Privacidad de la cuenta** de su app. Si no encuentra el mensaje de validación en su bandeja de entrada, compruebe también la carpeta de correo no deseado.
   Se muestra el estado de privacidad de la cuenta validada.

En caso de detectarse filtraciones en cualquiera de sus cuentas, le recomendamos que cambie su contraseña lo antes posible. Para crear una contraseña realmente segura, siga estos consejos:

- Créela de por lo menos ocho caracteres de longitud.

- Utilice una combinación de mayúsculas y minúsculas.
- Incluya al menos un número o un símbolo, como por ejemplo #, @, % o !.

Una vez que haya protegido una cuenta que había sufrido una vulneración de la privacidad, puede confirmar los cambios marcando la filtración identificada como **Solucionada**. Para ello:

1. Toque en ··· junto a la vulneración que ha resuelto.
2. Toque **Marcar como resuelto**.

Cuando todas las filtraciones detectadas se hayan marcado como Solucionadas, la cuenta ya no aparecerá como objeto de filtraciones, al menos hasta que se vuelva a detectar una nueva filtración.

6.8. Preguntas más frecuentes

¿Cómo me protege Bitdefender Mobile Security for iOS contra virus y amenazas digitales?

Bitdefender Mobile Security for iOS proporciona protección absoluta contra todas las amenazas digitales y está especialmente diseñado para mantener sus datos confidenciales a salvo de miradas indiscretas.

Obtiene una gran cantidad de características de seguridad y privacidad avanzadas para su iPhone y iPad, además de muchas otras, como VPN y Protección web.

Bitdefender Mobile Security for iOS reacciona instantáneamente ante virus y malware sin sacrificar el rendimiento de su sistema.

¿Qué tipo de dispositivos y sistemas operativos cubre Bitdefender Mobile Security for iOS?

Bitdefender Mobile Security for iOS protegerá sus smartphones y tablets con iOS contra todas las amenazas digitales.

¿Por qué necesito Bitdefender Mobile Security for iOS en el sistema operativo de Apple?

Algunos de sus datos más personales se almacenan en su iPhone o iPad y necesita saber que están seguros en todo momento. Bitdefender Mobile Security for iOS proporciona protección absoluta contra amenazas digitales y se encarga de su privacidad online y de su información confidencial sin interferir en sus actividades cotidianas.

¿Obtengo una VPN con mi suscripción a Bitdefender Mobile Security for iOS?

Bitdefender Mobile Security for iOS viene con una versión básica de Bitdefender VPN que incluye gratuitamente una generosa cantidad de tráfico (200 MB/día, un total de GB al mes).

7. VPN

7.1. Qué es Bitdefender Total Security

La VPN sirve como un túnel entre su dispositivo y la red a la que se conecta para proteger su conexión, cifrar los datos mediante cifrado de grado militar y ocultar su dirección IP dondequiera que esté. Su tráfico se redirige a través de un servidor independiente; lo que hace que sea imposible que su ISP identifique su dispositivo, a través de la gran cantidad de otros dispositivos que utilizan nuestros servicios. Además, mientras esté conectado a Internet a través de Bitdefender VPN, podrá acceder a contenido que normalmente está restringido en áreas específicas.

> **Nota**
> Algunos países practican la censura de Internet y, por lo tanto, el uso de las VPN en su territorio está prohibido por la ley. Para evitar responsabilidades legales, puede que aparezca un mensaje de advertencia cuando trate de utilizar Bitdefender Total Security por primera vez. Al seguir haciendo uso de esa característica, confirma que es consciente de las regulaciones nacionales aplicables y de los riesgos a los que podría exponerse.

7.1.1. Protocolos de cifrado

A continuación se proporcionan los conjuntos de cifrado por defecto habilitados en el cliente y servidor Hydra. Los demás conjuntos de cifrado están inhabilitados.

Conjuntos de cifrado del cliente Hydra:

- ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

> **Nota**
> El conjunto del lado del servidor es mucho más restrictivo y tanto el cliente como el servidor Hydra rechazarán un modo que no sea GCM con AES. El servidor Hydra impone la prioridad de conjuntos de cifrado más fuertes del lado del servidor y rechazará el protocolo de enlace TLS si un cliente solicita un conjunto más débil. Esta lista también es configurable en tiempo de ejecución del lado del servidor.

7.2. Suscripciones de VPN

Con Bitdefender Total Security, puede optar por dos tipos de suscripciones:

- Las suscripción básica
- La suscripción Premium

7.2.1. Suscripción básica

Bitdefender Total Security ofrece de forma gratuita una cuota diaria de tráfico de 200 MB por dispositivo para proteger su conexión cuando lo necesite y le permite conectarse a una única ubicación que no se puede cambiar.

La suscripción básica está a disposición de cualquier usuario que descargue Bitdefender Total Security.

7.2.2. Suscripción Premium

Para obtener acceso ilimitado a todas las características incluidas en Bitdefender Total Security, actualice a la versión Premium. Los usuarios con una suscripción VPN Premium activa tienen tráfico protegido ilimitado y pueden conectarse a cualquiera de nuestros servidores en todo el mundo.

Hay dos planes disponibles para la suscripción Premium: mensual y anual.

- Plan mensual: con este plan, se le cobrará cada mes por los servicios Premium VPN. Puede anular su suscripción cuando lo desee.
- Plan anual: requiere un pago único que le otorga acceso a nuestros servicios Premium VPN durante todo un año.

7.2.3. Cómo actualizar a Premium VPN

La forma más fácil de actualizar a la versión Premium de Bitdefender Total Security es hacer clic en el botón **Actualizar** ubicado en la parte inferior de la interfaz principal. Elija el modelo de suscripción deseado y luego siga las instrucciones que aparecen en la pantalla.

Si ya tiene un código de activación, siga las instrucciones que se exponen a continuación:

- **Para usuarios de Windows**

  1. Haga clic en el icono Mi cuenta de la izquierda de la interfaz de VPN.
  2. Haga clic en **Añadir aquí**.
  3. Escriba el código recibido por correo electrónico y, a continuación, haga clic en el botón **Activar código**.

- **Para usuarios de macOS**

  1. Haga clic en el engranaje de la esquina superior derecha de la interfaz de VPN y seleccione **Mi cuenta**.
  2. Hacer clic **Agrégalo aquí**.
  3. Escriba el código recibido por correo electrónico, luego haga clic en el **codigo de activacion** botón.

- **Para usuarios de Android**

  1. Toque en el engranaje de la esquina superior derecha de la interfaz de VPN y seleccione **Mi cuenta**.
  2. Toque en **Añadir código**.
  3. Escriba el código recibido por correo electrónico, luego haga clic en el **codigo de activacion** botón.

- **Para usuarios de iOS**

  1. Toque la rueda dentada en la esquina superior derecha de la interfaz VPN y seleccione **Mi cuenta**.
  2. Grifo **Agregar código**.

3. Escriba el código recibido por correo electrónico, luego haga clic en el **codigo de activacion** botón.

7.3. Instalación

7.3.1. Preparándose para la instalación

Antes de instalar Bitdefender Total Security, complete estos preparativos para garantizar la instalación sin problemas:

- Asegúrese de que el dispositivo donde piensa instalar Bitdefender cumple los requisitos del sistema. Si el dispositivo no cumple con todos los requisitos del sistema, Bitdefender no se instalará o, si estuviera instalado, no funcionaría correctamente y provocaría demoras e inestabilidad en el sistema.
  Para ver la lista completa de todos los requisitos del sistema, consulte Requisitos del sistema (página 244)
- Inicie sesión en el dispositivo utilizando una cuenta de Administrador.
- Durante la instalación, se recomienda que su dispositivo esté conectado a Internet, incluso si la realiza desde un CD o DVD. Si hay disponibles versiones más recientes de los archivos de la aplicación incluidos en el paquete de instalación, Bitdefender puede descargarlas e instalarlas.

7.3.2. Requisitos del sistema

- **Para usuarios de Windows**
  - **Sistema operativo:** Windows 7 con Service Pack 1, Windows 8, Windows 8.1 Windows 10 y Windows 11
  - **Memoria (RAM):** 1 GB
  - **Espacio libre en disco:** 500 MB de espacio libre
  - **Net Framework:** versión mínima 4.5.2

    Importante
    El rendimiento del sistema puede verse afectado en dispositivos que tengan CPU de generaciones anteriores.
- **Para usuarios de macOS**

- **Sistema operativo:** macOS Sierra (10.12) o posterior
- **Espacio libre en disco:** 100 MB de espacio libre

- **Para usuarios de Android**
  - **Sistema operativo:** Android 5.0 o posterior
  - **Almacenamiento:** 100 MB
  - Una conexión de Internet activa

- **Para usuarios de iOS**
  - **Sistema operativo:** iOS 12 o posterior
  - **Almacenamiento en iPhone:** 50 MB
  - **Almacenamiento en iPad:** 100 MB
  - Una conexión a Internet activa

7.3.3. Instalación de Bitdefender Total Security

Para comenzar la instalación, siga las instrucciones correspondientes al sistema operativo que utilice:

- **Para usuarios de Windows**

  1. Para iniciar la instalación de Bitdefender Total Security en un PC con Windows, empiece por descargar el kit de instalación desde https://www.bitdefender.com/solutions/vpn/download o desde el mensaje de correo electrónico que recibió tras realizar su compra.
  2. Haga doble clic en el instalador que ha descargado para ejecutarlo.
  3. Elija Sí si se le presenta el cuadro de diálogo del Control de cuentas de usuario.
  4. Espere a que se complete la descarga.
  5. Seleccione el idioma del producto utilizando el menú desplegable del instalador.
  6. Marque la casilla de verificación “Confirmo que he leído y acepto el Acuerdo de suscripción y la Política de privacidad” y, a continuación, haga clic en **INICIAR LA INSTALACIÓN**.
  7. Espere a que finalice la instalación.

8. **INICIE SESIÓN** con su cuenta de Bitdefender Central. Si carece de una cuenta de Central, regístrese para obtenerla haciendo clic en el botón **CREAR CUENTA**.
9. Elija **Tengo un código de activación** si ha comprado una suscripción Premium VPN.
   De lo contrario, puede elegir **COMENZAR LA EVALUACIÓN** para probar el producto de forma gratuita durante siete días antes de comprometerse a pagarlo.
10. Escriba el código recibido por correo electrónico y, a continuación, haga clic en el botón **ACTIVAR PREMIUM**.
11. Tras una corta espera, Bitdefender Total Security queda instalado y listo para usarse en su equipo.

❍ **Para usuarios de macOS**

1. Para iniciar la instalación de Bitdefender Total Security en macOS, empiece por descargar el kit de instalación desde https://www.bitdefender.com/solutions/vpn/download o desde el mensaje de correo electrónico que recibió tras realizar su compra.
2. El instalador se guardará en el Mac. En la carpeta Descargas, haga doble clic en el archivo de paquete de .
3. Siga las instrucciones que aparecen en la pantalla. Elija **Continuar**.
4. Se le guiará por los pasos necesarios para instalar Bitdefender Total Security en su Mac. Haga clic dos veces en el botón **Continuar**.
5. Haga clic en **Aceptar** una vez leídos y aceptados los términos del acuerdo de licencia de software.
6. Haga clic en **Instalar**.
7. Introduzca un nombre de usuario y contraseña de administrador y, a continuación, haga clic en **Instalar el software**.
8. Se le notificará que se ha bloqueado una extensión de sistema firmada por Bitdefender. Esto no es un error, sino un mero control de seguridad. Haga clic en **Abrir preferencias de seguridad**.
9. Haga clic en el icono del candado para desbloquear.
   Introduzca un nombre y contraseña de administrador y, a continuación, pulse **Desbloquear**.

10. Haga clic en **Permitir** para cargar la extensión del sistema de BitdefenderBitdefender. Luego, cierre la ventana de Seguridad y privacidad y el instalador.

11. Acceda al icono del escudo en la barra de menús y, a continuación, **inicie sesión** con su cuenta de Bitdefender Central. Si carece de una cuenta de Central, regístrese para obtener una.

12. Elija tengo un **Código de activación** si ha comprado una suscripción Premium VPN.
    De lo contrario, puede elegir **INICIAR PRUEBA** para probar el producto de forma gratuita durante 7 días antes de comprometerse a pagarlo.

13. Escriba el código recibido por correo electrónico, luego haga clic en el **codigo de activacion** botón.

14. Tras una corta espera, Bitdefender Total Security queda instalado y listo para usarse en su Mac.

❍ **Para usuarios de Android**

1. Para instalar Bitdefender Total Security en Android, primero abra la aplicación **Google Play Store** en su smartphone o tablet.
2. Busque Bitdefender Total Security y seleccione esta app.
3. Toque en el botón **Instalar** y espere a que se complete la descarga.
4. Toque en **Abrir** para ejecutar la app.
5. Marque la casilla de verificación “Acepto el Acuerdo de suscripción y la Política de privacidad” y, a continuación, toque en **Continuar**.
6. **Inicie sesión** con su cuenta de Bitdefender Central. Si carece de una cuenta de Central, regístrese para obtenerla tocando en **Crear cuenta**.
7. Elija **Tengo un código de activación** si ha comprado una suscripción Premium VPN.
   De lo contrario, puede elegir Iniciar la versión de evaluación gratuita de siete días para probar el producto antes de comprometerse a pagarlo.
8. Escriba el código recibido por correo electrónico y, a continuación, toque en **Activar código**.

- **Para usuarios de iOS**

  1. Para instalar Bitdefender Total Security en iOS, primero abra la **App Store** en su iPhone o iPad.
  2. Buscar Bitdefender Total Security y seleccione esta aplicación.
  3. Toque en el icono **Obtener** y espere a que se complete la descarga.
  4. Grifo **Abierto** para ejecutar la aplicación.
  5. Marque la casilla de verificación **Acepto el Acuerdo de suscripción y la Política de privacidad** y, a continuación, toque en **Continuar**.
  6. **Inicie sesión** con su cuenta de Bitdefender Central. Si carece de una cuenta, regístrese para obtenerla tocando en **Crear cuenta**.
  7. Toque en **Permitir** si desea recibir notificaciones de Bitdefender Total Security.
  8. Elegir **tengo un codigo de activacion** si ha comprado una suscripción Premium VPN.
     De lo contrario, puede elegir Iniciar prueba de 7 días para probar el producto de forma gratuita durante 7 días antes de comprometerse a pagarlo.
  9. Escriba el código recibido por correo electrónico, luego toque **Codigo de activacion**.

7.4. Uso de Bitdefender VPN

7.4.1. Abrir Bitdefender VPN

- **Para Windows**
  Para acceder a la **interfaz principal de Bitdefender VPN**, utilice uno de los siguientes métodos:

  - **Desde la bandeja del sistema**
    Haga clic con el botón derecho en el ícono del escudo rojo de la bandeja del sistema y, a continuación, seleccione **Mostrar** en el menú.

  - **Desde la interfaz de Bitdefender**
    Si ya tiene instalado en su equipo con Windows algún producto de seguridad de Bitdefender, como Bitdefender Total Security o Bitdefender Antivirus Plus, puede abrir Bitdefender VPN desde allí:

1. Haga clic en **Privacidad** en la barra lateral izquierda de la interfaz de Bitdefender.
2. Haga clic en **Abrir VPN** en el panel de VPN.

- **Desde su Escritorio**
  Haga doble clic en el acceso directo de Bitdefender VPN presente en su Escritorio.

- **Para macOS**
  Puede abrir la aplicación Bitdefender VPN haciendo clic en el icono de la barra de menús en la parte superior derecha de la pantalla.
  Si no encuentra el escudo de Bitdefender en la barra de menús, use el Launchpad o Finder de su Mac para recuperarlo:

  - **Desde Launchpad**

    1. Pulse **F4** en su teclado para entrar en el Launchpad de su Mac.
    2. Examine las páginas de las aplicaciones instaladas hasta que localice la de Bitdefender VPN. Como alternativa, puede escribir **Bitdefender VPN** en el Launchpad para filtrar sus resultados.
    3. Cuando haya localizado la aplicación Bitdefender VPN, haga clic en su icono para anclarlo a la barra de menús.

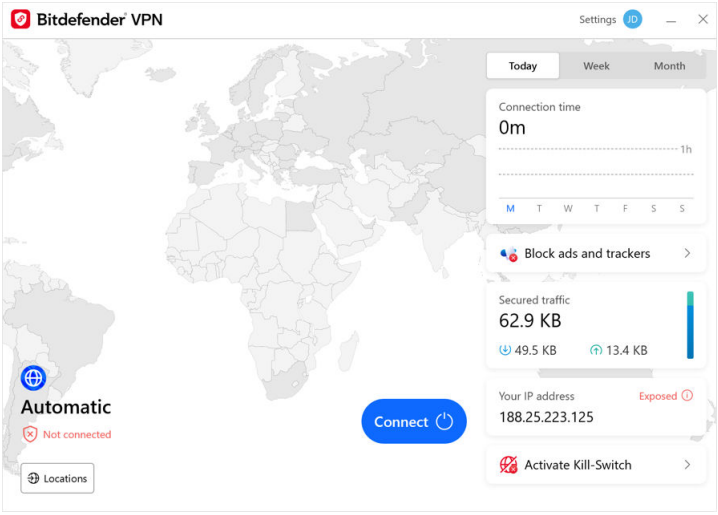
  - **Desde Finder**

    1. Haga clic en **Finder** en la parte inferior izquierda del Dock (Finder es el icono del cuadrado azul con una cara sonriente).
    2. A continuación, haga clic en **Ir** en la parte superior izquierda de la pantalla, en la barra de menús.
    3. Seleccione **Aplicaciones** en el menú para acceder a la carpeta Aplicaciones de su Mac.
    4. Desde la carpeta Aplicaciones, abra la carpeta **Bitdefender** y, a continuación, haga doble clic en la aplicación de **Bitdefender VPN**.

> **Nota**
> Para acceder a Bitdefender VPN en sus dispositivos móviles Android o iOS, basta con que abra la aplicación Bitdefender VPN tras haberla instalado.

7.4.2. Cómo conectarse a Bitdefender Total Security

La interfaz de VPN muestra el estado de la app: conectada o desconectada. Para los usuarios con la versión gratuita, Bitdefender configura automáticamente la ubicación del servidor a la más apropiada, mientras que los usuarios prémium tienen la posibilidad de cambiar la ubicación del servidor al que deseen conectarse escogiéndola en la lista de Ubicaciones virtuales. Para conectarse o desconectarse, haga clic en el botón de encendido de la interfaz de VPN.



- **Para Windows:** El icono del área de notificación muestra una marca de verificación verde cuando la VPN está conectada y una negra cuando no lo está. Mientras permanece conectado a una ubicación seleccionada manualmente, la interfaz principal muestra la dirección IP.
- **Para macOS:** El icono de la barra de menús aparece en negro cuando la VPN está conectada y en blanco cuando no lo está. Haga clic en el botón circular en medio de la interfaz y espere a que se establezca la conexión.
- **Para iOS y Android:** Para conectarse a Bitdefender VPN en iOS, iPadOS y Android, haga lo siguiente:

- **En la app de Bitdefender VPN:** Para conectarse o desconectarse, toque el botón de encendido de la interfaz de VPN. Se muestra el estado de Bitdefender VPN.
- **En la app Bitdefender Mobile Security:**
  1. Acceda al icono VPN en la barra de navegación inferior de Bitdefender Mobile Security.
  2. Toque **CONECTAR** siempre que desee permanecer protegido mientras se conecte a redes inalámbricas inseguras. Toque **DESCONECTAR** cuando desee desactivar la conexión.

7.4.3. Cómo conectarse a un servidor diferente

Con una suscripción Premium, Bitdefender Total Security le permite conectarse a cualquiera de nuestros servidores de todo el mundo en cualquier momento. Para ello, tendrá que hacer lo siguiente:

1. Abra la app Bitdefender Total Security.
2. Toque en el botón **Ubicación virtual** de la zona inferior de la interfaz.
3. Seleccione el país que desee.
4. Haga clic en el botón **Conectarse a [país de su elección]** de la zona inferior de la interfaz.

- El icono de la bandeja del sistema muestra una marca de verificación verde cuando la VPN está conectada.
- La dirección IP del servidor virtual se muestra en la pantalla de inicio mientras está conectado a Bitdefender VPN.
- En el panel principal también se muestra un resumen de su tiempo de conexión, la cantidad de tráfico seguro y las últimas 5 ubicaciones a las que se conectó.

7.5. Ajustes y características de Bitdefender Total Security

7.5.1. Acceso a los ajustes

Para acceder a los ajustes de Bitdefender Total Security, deberá seguir los pasos que se describen a continuación:

- **En Windows**
  1. Abra la aplicación de Bitdefender Total Security en su dispositivo haciendo doble clic en su icono en la bandeja del sistema o haciendo clic con el botón derecho sobre él y seleccionando Mostrar.
  2. Haga clic en el botón de **Ajustes** (representado por un engranaje) de la izquierda de la interfaz.

- **En macOS**
  1. Abra la aplicación de Bitdefender Total Security en su dispositivo macOS haciendo clic en su icono en la barra de menús.
  2. Haga clic en el botón del engranaje de la esquina superior derecha de la interfaz de Bitdefender Total Security y seleccione Ajustes.

- **En Android**
  1. Abra la aplicación de Bitdefender Total Security en su dispositivo.
  2. Haga clic en el botón del engranaje de la esquina superior derecha de la interfaz de Bitdefender Total Security.

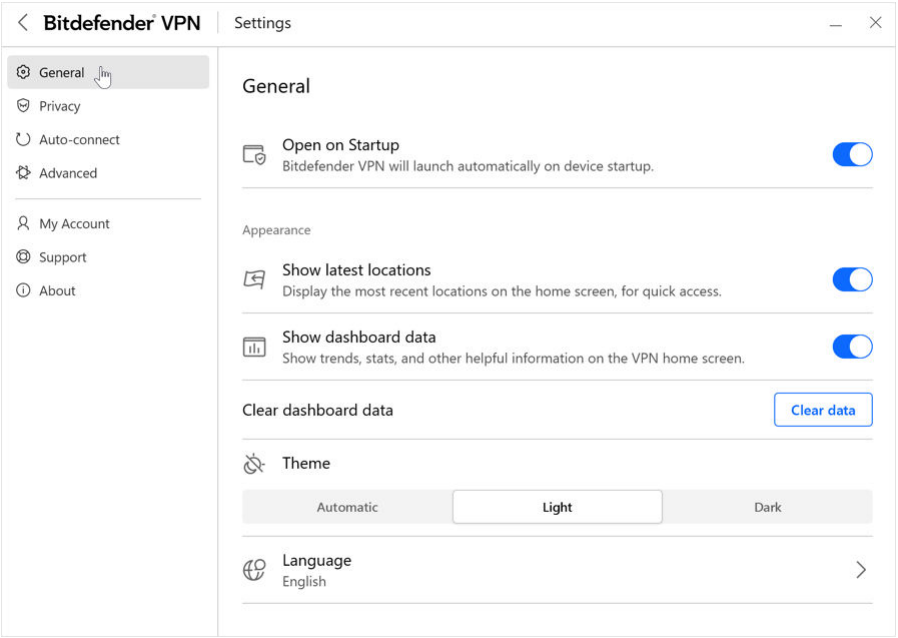
- **En iOS**
  1. Abre el Bitdefender Total Security aplicación en su dispositivo.
  2. Haga clic en el botón de la rueda dentada en la esquina superior derecha de la Bitdefender Total Security interfaz.

7.5.2. General

Aquí podrás modificar lo siguiente:

- **Abrir al iniciar**– Bitdefender VPN se iniciará automáticamente al iniciar el dispositivo.
- **Mostrar las últimas ubicaciones**– Muestra las ubicaciones más recientes en la pantalla de inicio, para un acceso rápido.
- **Mostrar datos del panel** – Muestra tendencias, estadísticas y otra información útil en la pantalla de inicio de VPN.
- **Borrar datos del panel**– Se borrarán todos los datos de su panel y se restablecerán todos los contadores.

- **Tema**– Tema claro/oscuro
- **Idioma**– Cambiar el idioma de Bitdefender VPN.
- **Notificaciones**– Administre sus preferencias de notificaciones.
- **Ayude a mejorar Bitdefender VPN**– Envíe informes anónimos de productos para ayudarnos a mejorar su experiencia.
- **Restablecer todos los ajustes**– Restablezca la VPN a su configuración original sin reinstalarla.



7.5.3. Características

Privacidad

Conmutador de interrupción de Internet

El conmutador de interrupción es una nueva característica implementada en Bitdefender Total Security. Cuando está habilitada, esta característica interrumpe todo el tráfico de Internet si se suspende la conexión VPN. Tan pronto como vuelva a estar online, se restablecerá la conexión VPN.

Para activar el conmutador de interrupción, siga los pasos que se exponen a continuación:

- **en ventanas**
  1. Abra la aplicación de Bitdefender Total Security en su dispositivo haciendo doble clic en su icono en la bandeja del sistema o haciendo clic con el botón derecho sobre él y seleccionando **Mostrar**.
  2. Clickea en el **Ajustes** botón (representado por una rueda dentada) en el lado izquierdo de la interfaz.
  3. Seleccione **Avanzado**.
  4. Habilite la opción **Conmutador de interrupción de Internet**.
- **En Android**
  1. Abre el Bitdefender Total Security aplicación en su dispositivo.
  2. Haga clic en el botón de la rueda dentada en la esquina superior derecha de la Bitdefender Total Security interfaz.
  3. En **Ajustes**, habilite la opción **Conmutador de interrupción**.
- **En iOS**
  1. Abre el Bitdefender Total Security aplicación en su dispositivo.
  2. Haga clic en el botón de la rueda dentada en la esquina superior derecha de la Bitdefender Total Security interfaz.
  3. Bajo **Ajustes**, habilitar el **Kill-Switch** opción.

> **Nota**
> Esta característica también está disponible para dispositivos macOS con sistemas operativos 10.15.4 o posteriores.

Bloqueador de anuncios y Anti-tracker

Estas características están pensadas para ayudarle a mantener la privacidad y disfrutar de la web sin molestos anuncios ni empresas que le vigilen. Ayudan a bloquear anuncios y detener rastreadores online.

Bloqueador de anuncios

El **Bloqueador de anuncios** se utiliza para bloquear anuncios, ventanas emergentes, anuncios de vídeo con sonido o banners publicitarios

mientras navega. Esto contribuye a que los sitios web se carguen más rápidamente y se vean más despejados, además de resultar más seguro interactuar con ellos.

Para habilitar el Bloqueador de anuncios:

1. Localice la característica **Bloqueador de anuncios y Anti-tracker** en **Ajustes**.
2. Pase el conmutador a la posición **ACTIVADO**.

Anti-tracker

El **Anti-tracker** se utiliza para bloquear los rastreadores que los anunciantes configuran para seguirle y trazar su perfil online. Es posible que algunos sitios web no funcionen correctamente si se bloquean los rastreadores. Añadir su URL a la lista blanca podría solucionar este problema.

Para habilitar el Anti-tracker:

1. Localiza el **Bloqueador de anuncios y Antitracker** característica en **Ajustes**.
2. Cambie el interruptor a la **EN** posición.

Lista blanca

Es posible que algunos sitios web no se carguen correctamente si bloquea su código de rastreo y sus anuncios. Añadir las URL de estos dominios concretos a la lista blanca puede solucionar este problema, pero tenga en cuenta que, mientras navegue por estos sitios web, verá anuncios y su código de rastreo permanecerá activo.

Añada el sitio web al que desea permitir mostrar anuncios y utilizar rastreadores de la siguiente manera:

1. Localiza el **Bloqueador de anuncios y Antitracker** característica en **Ajustes**.
2. Haga clic en el enlace **Administrar**. A continuación, acceda a la sección Lista blanca de la ventana y haga clic en el enlace **Administrar** correspondiente.
3. Haga clic en **Añadir sitio web** e introduzca la URL deseada.

Conectar automáticamente

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.

Para protegerle de los peligros de los puntos de acceso inalámbricos públicos inseguros o sin cifrar, Bitdefender Total Security incluye una característica de conexión automática. Esto significa que Bitdefender Total Security puede activarse automáticamente en ciertas situaciones, dependiendo de sus preferencias y del sistema operativo en que se esté ejecutando.

- En **Windows**, la característica de conexión automática puede habilitarse en las siguientes situaciones:
  - **Inicio:** Conectar la VPN al inicio de Windows.
  - **Conexión Wi-Fi insegura:** Usar la VPN siempre que se conecte a redes Wi-Fi públicas o inseguras.
  - **Aplicaciones punto a punto:** Conectar la VPN cuando inicie una aplicación de uso compartido de archivos punto a punto.
  - **Aplicaciones y dominios:** Utilizar siempre la VPN para determinadas aplicaciones y sitios web.

    Nota

    1. Haga clic en el enlace **Administrar**.
    2. Busque la ubicación de la aplicación para la que desea utilizar la VPN, seleccione su nombre y, a continuación, haga clic en **Añadir**.

  - **Categorías de sitios web:** Conectar la VPN cuando visite determinadas categorías de sitios web. Bitdefender VPN puede conectarse automáticamente para las siguientes categorías de sitios web:
    - Finanzas
    - Pagos online

- Salud
- Intercambio de archivos
- Citas Online
- Contenido para adultos

> **Nota**
> Para cada categoría, puede seleccionar un servidor diferente al que se conecte la VPN.

- En **macOS**, la característica de conexión automática puede habilitarse en las siguientes situaciones:
  - **Inicio:** Conectar la VPN al inicio de macOS.
  - **Wi-Fi no seguro:** Utilice la VPN cada vez que se conecte a redes Wi-Fi públicas o no seguras.
  - **Aplicaciones punto a punto:** Conéctese a la VPN cuando inicie una aplicación para compartir archivos punto a punto.
  - **Aplicaciones:** Conectar siempre la VPN para determinadas aplicaciones.
- En **iOS** y **Android**, Bitdefender Total Security puede configurarse para conectarse automáticamente solo cuando esté conectado a una red Wi-Fi pública o insegura.

Avanzado

Túnel dividido

El túnel dividido de red privada virtual (VPN) permite enrutar parte del tráfico de su aplicación o dispositivo a través de una VPN cifrada mientras que las otras aplicaciones o dispositivos acceden directamente a Internet. Esto es especialmente útil para beneficiarse de servicios que funcionan mejor cuando conocen su ubicación y, sin embargo, disfrutar de un acceso seguro a comunicaciones y datos potencialmente confidenciales.

Al habilitar la característica de **túnel dividido**, las aplicaciones y sitios web seleccionados se saltarán la VPN y accederán directamente a Internet.

Para administrar las aplicaciones y los sitios web que omiten la VPN, haga lo siguiente:

1. Haga clic en el enlace **Administrar** una vez que haya habilitado la característica.
2. Haga clic en el botón **Añadir**.
3. Busque la ubicación de la aplicación en cuestión o introduzca la URL del sitio web deseado y, a continuación, haga clic en **Añadir**.

> **Nota**
> Al añadir un sitio web, se omitirá el uso de VPN para todo el dominio, incluyendo sus subdominios.

> **Importante**
> En dispositivos **macOS**, la característica de túnel dividido solo se aplica a sitios web.

Optimizador de tráfico de aplicaciones

El Optimizador de tráfico de aplicaciones de Bitdefender Total Security le permite dar prioridad al tráfico de las aplicaciones más importantes de su dispositivo sin exponer su conexión a riesgos para la privacidad. Las VPN redirigen el tráfico de Internet a través de un túnel seguro al tiempo que utilizan sólidos algoritmos de cifrado para protegerlo.

No obstante, esta combinación de técnicas puede acarrear algunos inconvenientes, principalmente en lo que se refiere a la velocidad de conexión. Existen diversos factores que pueden ralentizar la conexión, como son la distancia al servidor al que se está conectando, la congestión de la red y el uso de un elevado ancho de banda. Si cree que, en ocasiones, Bitdefender Total Security sobrecarga innecesariamente su conexión y le ocasiona demoras, puede que haya una solución mejor que desconectarse.

¿Cómo funciona el Optimizador de tráfico de aplicaciones?

Ciertas aplicaciones y servicios, como las plataformas de streaming, los clientes de torrent y los juegos, exigen más ancho de banda. Por ello, su uso constante podría afectar la velocidad de su conexión a Internet. Enrutar su tráfico a través de un túnel VPN ya somete su conexión a una relativa demora, de modo que tensionarla más podría degradar notablemente su experiencia online.

La característica Optimizador de tráfico de aplicaciones de Bitdefender Total Security puede ayudarle a lidiar con las demoras de la conexión VPN dando prioridad a la aplicación que usted desee. Esta característica le permite decidir qué aplicaciones han de recibir la mayor parte del tráfico y, posteriormente, asigna los recursos en consecuencia. Por ejemplo, si se encuentra en una reunión y se da cuenta de que la calidad de la llamada no está a la altura, el Optimizador de tráfico de aplicaciones le permite priorizar el tráfico hacia la aplicación de videoconferencia para mejorar los resultados.

Normalmente, los usuarios de VPN recurrirían a cerrar todos los procesos que interfieran en su dispositivo o incluso a inhabilitar su conexión VPN para aumentar la velocidad de Internet. El Optimizador de tráfico de aplicaciones le permite disfrutar de una protección ininterrumpida de su privacidad sin comprometer por ello su velocidad de conexión.

Uso del Optimizador de tráfico de aplicaciones

Actualmente, esta característica solo está disponible en dispositivos Windows y le permite priorizar el tráfico de hasta tres aplicaciones.

Para habilitarla y configurarla con el mínimo esfuerzo, siga los pasos que se exponen a continuación:

1. Lance la aplicación Bitdefender VPN en su equipo con Windows.
2. Haga clic en el botón de la barra lateral para acceder a los ajustes de la VPN.
3. Acceda a la pestaña **General** y habilite la característica **Optimizador de tráfico de aplicaciones**. El color del conmutador pasará de gris a azul.

Para administrar las aplicaciones priorizadas por esta característica, haga lo siguiente:

1. Haga clic en el**Administrar**enlace.
2. Busque la ubicación de la aplicación para la que desea optimizar el tráfico, seleccione su nombre y, a continuación, haga clic en **Añadir**. La aplicación aparecerá en la sección **Con prioridad**.

> **Nota**
> Como alternativa, si ha abierto recientemente la aplicación que desea priorizar, pulse el botón + en la ventana del Optimizador de tráfico de aplicaciones.

3. Desconéctese y vuelva a conectarse a Bitdefender VPN tras añadir o eliminar aplicaciones de la lista.

Para eliminar una aplicación del Optimizador de tráfico de aplicaciones, basta con hacer clic en el icono junto a su nombre.

> **Nota**
> El Optimizador de tráfico de aplicaciones no está disponible en macOS.

Protocolo

Aquí puede elegir el tipo de protocolo que desea utilizar para la transferencia de datos. Las siguientes opciones están disponibles:

- **Automático** - Bitdefender VPN seleccionará el protocolo óptimo para su dispositivo y red específicos.
- **Catapulta de hidra** - Rápido y seguro, ideal para streaming y juegos.
- **OpenVPN UDP** - Optimizado para velocidades rápidas. Sin embargo, este protocolo no es tan confiable en términos de pérdida de datos como otros protocolos de la lista.
- **OpenVPN TCP** - Diseñado para brindar confiabilidad. Garantiza que sus datos se entreguen en su totalidad, pero no es tan rápido como OpenVPN UDP.
- **guardacables** - Protocolo más nuevo, que proporciona una gran seguridad y un alto nivel de rendimiento.

doble salto

Con esta función puedes administrar los servidores a través de los cuales enviar y cifrar doblemente tu tráfico de Internet. Tus datos pasarán a través de dos servidores VPN en lugar de uno, lo que dificultará el seguimiento de tu actividad en Internet.

Nota

Solo puedes agregar un total de 5 ubicaciones de doble salto. Sin embargo, puede eliminar los saltos dobles personalizados de su lista y crear otros en cualquier momento.

Importante

El uso de servidores ubicados en diferentes continentes en el mismo doble salto puede ralentizar la velocidad de su conexión.

7.6. Desinstalar Bitdefender Total Security

El procedimiento para eliminar Bitdefender Total Security es similar al empleado para desinstalar otros programas de su equipo:

- **Desinstalar Bitdefender Total Security de dispositivos Windows**
  - En **Windows 7**:
    1. Haga clic en **Inicio**, acceda al **Panel de control** y haga doble clic en **Programas y características**.
    2. Busque **Bitdefender Total Security** y seleccione **Desinstalar**. Espere a que el proceso de desinstalación se complete.
  - 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. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**. Espere a que se complete el proceso de desinstalación.
  - En **Windows 10** y **Windows 11**:
    1. Haga clic en **Inicio** y, a continuación, haga clic en **Ajustes**.
    2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
    3. Encontrar **Bitdefender Total Security** y seleccione **Desinstalar**.

4. Haga clic en **Desinstalar** para confirmar su elección.
   Espere a que se complete el proceso de desinstalación.

- **Desinstalar de dispositivos macOS**
  1. Haga clic en **Ir** en la barra de menús y seleccione **Aplicaciones**.
  2. Haga doble clic en la carpeta **Bitdefender**.
  3. Ejecute **BitdefenderUninstaller**.
  4. En la nueva ventana, marque la casilla de verificación junto a **Bitdefender Total Security** y, a continuación, haga clic en **Desinstalar**.
  5. Escriba un nombre de cuenta de administrador y una contraseña válidos y luego haga clic en **OK**.
  6. Por último, se le notificará que Bitdefender Total Security se ha desinstalado correctamente. Haga clic en **Cerrar**.

- **Desinstalar de dispositivos Android**
  1. Abra la app de **Play Store**.
  2. Busque **Bitdefender Total Security**.
  3. En la página de la tienda de aplicaciones Bitdefender Total Security, seleccione **Desinstalar**.
  4. Confirme tocando en **OK**.

- **Desinstalar de dispositivos iOS**
  1. Toque y mantenga pulsado el icono de la app de Bitdefender Total Security.
  2. Seleccione **Eliminar app**.
  3. Toque **Eliminar**.

7.7. Preguntas frecuentes

¿Cuándo debo usar Bitdefender VPN?

Ha de tener cuidado cuando acceda, descargue o cargue contenidos en Internet. Para asegurarse de que se mantiene a salvo mientras navega por la web, le recomendamos que use la VPN cuando:

- Desee conectarse a redes inalámbricas públicas.
- Desee acceder a contenidos que normalmente están restringidos en zonas concretas, sin importar si está en su hogar o en el extranjero.
- Desee mantener la privacidad de sus datos personales (nombres de usuario, contraseñas, direcciones de correo, información de tarjetas de crédito, etc.).
- Desee ocultar su dirección IP.

¿Puedo elegir una ciudad con Bitdefender VPN?

Sí. Ahora, Bitdefender VPN para Windows, macOS, iOS y Android permite seleccionar una ciudad concreta. Esta es la lista de ciudades disponibles actualmente:

- **EE. UU.:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Ángeles, Miami, Nueva York, Newark, Phoenix, Portland, San José, Seattle y Washington
- **Canadá:** Montreal, Toronto y Vancouver
- **Reino Unido:** Londres y Mánchester

¿Se puede instalar Bitdefender VPN como app independiente?

La app de VPN se instala automáticamente junto con su solución de seguridad de Bitdefender. También puede instalarse como una app independiente desde la página del producto en Google Play Store y App Store.

¿Compartirá Bitdefender mi dirección IP y mis datos personales con terceros?

No, con Bitdefender VPN su privacidad está garantizada al 100 %. Nadie (agencias de publicidad, proveedores de Internet, empresas de seguros, etc.) tendrá acceso a sus registros online.

¿Qué algoritmo de cifrado utiliza?

Bitdefender VPN utiliza el protocolo Hydra en todas las plataformas, cifrado AES de 256 bits o el mayor cifrado disponible que sea compatible tanto con el cliente como con el servidor, con sistema de secreto perfecto hacia delante. Esto significa que se generan claves de cifrado para cada nueva sesión de VPN y se borran de la memoria al finalizarla.

¿Puedo acceder a contenidos restringidos geográficamente?

Con Premium VPN tiene acceso a una amplia red de ubicaciones virtuales de todo el mundo.

¿Disminuirá la duración de la batería de mi dispositivo?

Bitdefender VPN está diseñado para proteger sus datos personales, ocultar su dirección IP mientras está conectado a redes inalámbricas inseguras y acceder a contenidos restringidos en ciertos países. Para evitar el consumo innecesario de la batería de su dispositivo, le recomendamos que use VPN solo cuando lo necesite y que prescinda de él cuando no esté conectado.

¿Por qué ralentiza la VPN mi conexión a Internet?

Bitdefender VPN se ha diseñado para ofrecer una rápida navegación por la web. Dependiendo de la distancia entre su ubicación real y la del servidor al que elija conectarse, cabe esperar cierta disminución de la velocidad, pero casi siempre es tan poca que pasa desapercibida durante una actividad online normal. Además, disponemos de una de las infraestructuras de VPN más rápidas del mundo. Si no es imprescindible que se conecte desde su ubicación a un servidor lejano (por ejemplo, desde España hasta Estados Unidos), le recomendamos que permita que la VPN se conecte automáticamente al servidor más cercano o que encuentre un servidor más próximo a su ubicación actual.

8. OBTENIENDO AYUDA

8.1. Solicitando Ayuda

Bitdefender proporciona a sus clientes un nivel sin igual de soporte técnico rápido y preciso. Si tiene cualquier problema o alguna pregunta sobre su producto Bitdefender, dispone de varios recursos online para encontrar una solución o una respuesta. Además, puede ponerse en contacto con el equipo de Atención al Cliente de Bitdefender. Nuestros representantes de soporte técnico responderán a sus preguntas con diligencia y le proporcionarán la asistencia que necesite.

8.2. Recursos Online

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

- Centro de soporte de Bitdefender:
  https://www.bitdefender.es/consumer/support/
- La comunidad de expertos de Bitdefender:
  https://community.bitdefender.com/es/
- Ciberpedia de Bitdefender:
  https://www.bitdefender.com/cyberpedia/

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

8.2.1. Centro de soporte de Bitdefender

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

El Centro de soporte de 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 la información que necesitan. Todas las solicitudes válidas de información o informes de errores procedentes de los clientes acaban finalmente 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 de Bitdefender está disponible en cualquier momento en la siguiente dirección: https://www.bitdefender.es/consumer/support/.

8.2.2. La comunidad de expertos de Bitdefender

La comunidad de expertos es un entorno en el que los usuarios, entusiastas y fanes de Bitdefender pueden participar, intercambiar ideas, apoyarse mutuamente y compartir sus conocimientos y soluciones. Además, es un lugar de creación de ideas y aporta valiosos comentarios a nuestros equipos de desarrollo. Los miembros de esta comunidad son usuarios experimentados de Bitdefender que se complacen en ayudar a otros en su tiempo libre. Con su inmensa contribución y su genuino esfuerzo de voluntariado, hemos creado una base de conocimientos en la que los usuarios pueden hallar respuestas y orientación, pero con un toque humano.

Aquí encontrará interesantes conversaciones con gente que usa Bitdefender en sus dispositivos. La comunidad establece una auténtica conexión entre sus miembros y hace oír su voz. Es un lugar donde se alienta la participación sabiendo que su opinión y aporte serán respetados y apreciados. Como valioso contribuyente, nos esforzamos por ofrecer un nivel sin igual de soporte técnico rápido y preciso y deseamos aproximarnos a nuestros usuarios. Con este propósito en mente hemos diseñado nuestra comunidad.

Puede encontrar la página web de nuestra comunidad de expertos aquí:

https://community.bitdefender.com/es/

8.2.3. Ciberpedia de Bitdefender

Bitdefender Cyberpedia contiene toda la información que necesita conocer sobre las últimas amenazas digitales. Aquí es donde los expertos de Bitdefender dan a conocer consejos y trucos para protegerse contra piratas informáticos, vulneraciones de datos, robos de identidad e intentos de suplantación en las redes sociales.

En el siguiente enlace puede encontrar la página web de Bitdefender Cyberpedia:

https://www.bitdefender.com/cyberpedia/.

8.3. Información de contacto

La comunicación eficiente es la clave para un negocio exitoso. Desde 2001, BITDEFENDER ha establecido una reputación incuestionable al esforzarse constantemente por mejorar la comunicación para superar las expectativas de nuestros clientes y socios. Si tiene alguna pregunta, no dude en contactarnos directamente a través de nuestro Centro de soporte de Bitdefender (página 265).

https://www.bitdefender.es/consumer/support/

8.3.1. Distribuidores locales

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

Para encontrar un distribuidor de Bitdefender en su país:

1. Ir a https://www.bitdefender.com/partners/localizador-de-socios.html.
2. Elija su país y ciudad mediante las opciones correspondientes.

GLOSARIO

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.

ActiveX

ActiveX es un modelo para escribir programas para que otros programas y el sistema operativo puedan llamarlos. La tecnología ActiveX se usa con Microsoft Internet Explorer para crear páginas web interactivas que se ven y se comportan como programas de computadora, en lugar de páginas estáticas. Con ActiveX, los usuarios pueden hacer o responder preguntas, usar botones e interactuar de otras formas con la página web. Los controles ActiveX a menudo se escriben usando Visual Basic. Active X se destaca por una completa falta de controles de seguridad; los expertos en seguridad informática desaconsejan su uso a través de internet.

Amenaza Persistente Avanzada

La amenaza persistente avanzada (APT) explota las vulnerabilidades de los sistemas para robar información importante y entregarla a la fuente. Grandes grupos, como organizaciones, empresas o gobiernos, son el blanco de esta amenaza. El objetivo de una amenaza persistente avanzada es pasar desapercibida durante mucho tiempo y poder monitorear y recopilar información importante sin dañar las máquinas objetivo. El método utilizado para inyectar la amenaza en la red es a través de un archivo PDF o un documento de Office que parezca inofensivo para que cada usuario pueda ejecutar los archivos.

publicidad

El adware a menudo se combina con una aplicación host que se proporciona sin cargo siempre que el usuario acepte el adware. Debido a que las aplicaciones de adware generalmente se instalan después de que el usuario haya aceptado un acuerdo de licencia que establece el propósito de la aplicación, no se comete ningún delito. Sin embargo, los anuncios emergentes pueden convertirse en una molestia y, en algunos

casos, degradar el rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas de privacidad para los usuarios que no conocían completamente los términos del acuerdo de licencia.

Archivo

Disco, cinta o directorio conteniendo ficheros almacenados.

Un archivo que contiene uno o más archivos en un formato comprimido.

Puerta trasera

Un agujero en la seguridad de un sistema dejado deliberadamente por diseñadores o mantenedores. La motivación de tales agujeros no siempre es siniestra; algunos sistemas operativos, por ejemplo, vienen listos para usar con cuentas privilegiadas destinadas a los técnicos de servicio de campo o los programadores de mantenimiento del proveedor.

Sector de arranque

Un sector al comienzo de cada disco que identifica la arquitectura del disco (tamaño del sector, tamaño del clúster, etc.). Para los discos de inicio, el sector de arranque también contiene un programa que carga el sistema operativo.

virus de arranque

Una amenaza que infecta el sector de arranque de un disco fijo o disquete. Un intento de arrancar desde un disquete infectado con un virus del sector de arranque hará que la amenaza se active en la memoria. Cada vez que inicie su sistema a partir de ese momento, tendrá la amenaza activa en la memoria.

red de bots

El término “botnet” se compone de las palabras “robot” y “red”. Los botnets son dispositivos conectados a Internet infectados con amenazas y se pueden usar para enviar correos electrónicos no deseados, robar datos, controlar de forma remota dispositivos vulnerables o propagar spyware, ransomware y otros tipos de amenazas. Su objetivo es infectar el mayor número posible de dispositivos conectados, como PC, servidores, dispositivos móviles o IoT pertenecientes a grandes empresas o industrias.

Navegador

Abreviatura de navegador web, una aplicación de software utilizada para localizar y mostrar páginas web. Los navegadores populares incluyen Microsoft Internet Explorer, Mozilla Firefox y Google Chrome. Estos son navegadores gráficos, lo que significa que pueden mostrar gráficos además de texto. Además, la mayoría de los navegadores modernos pueden presentar información multimedia, incluidos sonido y video, aunque requieren complementos para algunos formatos.

Ataque de fuerza bruta

Ataque de adivinación de contraseñas utilizado para ingresar en un sistema informático ingresando posibles combinaciones de contraseñas, en su mayoría comenzando con la contraseña más fácil de adivinar.

Línea de comando

En una interfaz de línea de comandos, el usuario escribe los comandos en el espacio provisto directamente en la pantalla usando el lenguaje de comandos.

Galletas

Dentro de la industria de Internet, las cookies se describen como pequeños archivos que contienen información sobre computadoras individuales que los anunciantes pueden analizar y usar para rastrear sus intereses y gustos en línea. En este ámbito, la tecnología de cookies aún se está desarrollando y la intención es orientar los anuncios directamente a lo que ha dicho que son sus intereses. Es un arma de doble filo para muchas personas porque, por un lado, es eficiente y pertinente, ya que solo ve anuncios sobre lo que le interesa. Por otro lado, implica realmente "rastrear" y "seguir" a dónde va y lo que haces clic. Comprensiblemente, existe un debate sobre la privacidad y muchas personas se sienten ofendidas por la noción de que se les considera un "número SKU" (ya sabe, el código de barras en la parte posterior de los paquetes que se escanea en la línea de pago del supermercado) . Si bien este punto de vista puede ser extremo, en algunos casos es exacto.

Ciberacoso

Cuando compañeros o extraños están cometiendo actos abusivos contra los niños con el propósito de lastimarlos físicamente. Para dañar emocionalmente, los agresores envían mensajes crueles o fotos poco favorecedoras, lo que hace que sus víctimas se aíslen de los demás o se sientan frustradas.

Ataque de diccionario

Los ataques de adivinación de contraseñas solían entrar en un sistema informático ingresando una combinación de palabras comunes para generar posibles contraseñas. El mismo método se utiliza para adivinar las claves de descifrado de mensajes o documentos cifrados. Los ataques de diccionario tienen éxito porque muchas personas se inclinan por elegir contraseñas cortas y de una sola palabra que sean fáciles de adivinar.

Disco duro

Es una máquina que lee y escribe datos en un disco. Una unidad de disco duro lee y escribe discos duros. Una unidad de disquete accede a disquetes. Las unidades de disco pueden ser internas (alojadas dentro de una computadora) o externas (alojadas en una caja separada que se conecta a la computadora).

Descargar

Para copiar datos (generalmente un archivo completo) desde una fuente principal a un dispositivo periférico. El término se usa a menudo para describir el proceso de copiar un archivo de un servicio en línea a la propia computadora. Descargar también puede referirse a copiar un archivo desde un servidor de archivos de red a una computadora en la red.

Correo electrónico

Correo electrónico. Un servicio que envía mensajes en computadoras a través de redes locales o globales.

Eventos

Una acción u ocurrencia detectada por un programa. Los eventos pueden ser acciones del usuario, como hacer clic con el botón del mouse o presionar una tecla, o eventos del sistema, como quedarse sin memoria.

hazañas

Una forma de aprovechar diferentes errores o vulnerabilidades que están presentes en una computadora (software o hardware). Por lo tanto, los piratas informáticos pueden obtener el control de las computadoras o las redes.

Falso positivo

Ocurre cuando un escáner identifica un archivo como infectado cuando en realidad no lo está.

Extensión de nombre de archivo

La parte de un nombre de archivo, después del punto final, que indica el tipo de datos almacenados en el archivo. Muchos sistemas operativos utilizan extensiones de nombre de archivo, por ejemplo, Unix, VMS y MS-DOS. Por lo general, tienen de una a tres letras (algunos sistemas operativos tristes y antiguos no admiten más de tres). Los ejemplos incluyen "c" para código fuente C, "ps" para PostScript, "txt" para texto arbitrario.

Heurístico

Un método basado en reglas para identificar nuevas amenazas. Este método de escaneo no se basa en una base de datos de información de amenazas específica. La ventaja del análisis heurístico es que no se deja engañar por una nueva variante de una amenaza existente. Sin embargo, ocasionalmente puede reportar código sospechoso en programas normales, generando el llamado "falso positivo".

Tarro de miel

Un sistema informático de señuelo configurado para atraer a los piratas informáticos para que estudien la forma en que actúan e identifiquen los métodos heréticos que utilizan para recopilar información del sistema. Las empresas y corporaciones están más interesadas en implementar y utilizar trampas trampa para mejorar su estado general de seguridad.

IP

Protocolo de Internet: un protocolo enrutable en el conjunto de protocolos TCP/IP que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reensamblaje de paquetes IP.

Subprograma de Java

Un programa Java que está diseñado para ejecutarse solo en una página web. Para usar un subprograma en una página web, debe especificar el nombre del subprograma y el tamaño (largo y ancho, en píxeles) que puede utilizar el subprograma. Cuando se accede a la página web, el navegador descarga el applet de un servidor y lo ejecuta en la máquina del usuario (el cliente). Los applets se diferencian de las aplicaciones en que se rigen por un estricto protocolo de seguridad.

Por ejemplo, aunque los subprogramas se ejecutan en el cliente, no pueden leer ni escribir datos en la máquina del cliente. Además, los subprogramas están más restringidos para que solo puedan leer y escribir datos del mismo dominio desde el que se sirven.

registrador de teclas

Un keylogger es una aplicación que registra todo lo que escribes. Los keyloggers no son de naturaleza maliciosa. Se pueden usar para fines legítimos, como monitorear la actividad de los empleados o los niños. Sin embargo, los ciberdelincuentes los utilizan cada vez más con fines maliciosos (por ejemplo, para recopilar datos privados, como credenciales de inicio de sesión y números de seguridad social).

Virus de macros

Un tipo de amenaza informática que se codifica como una macro incrustada en un documento. Muchas aplicaciones, como Microsoft Word y Excel, admiten potentes lenguajes de macros. Estas aplicaciones le permiten incrustar una macro en un documento y hacer que la macro se ejecute cada vez que se abre el documento.

cliente de correo

Un cliente de correo electrónico es una aplicación que le permite enviar y recibir correo electrónico.

Memoria

Áreas de almacenamiento interno en la computadora. El término memoria identifica el almacenamiento de datos que viene en forma de chips, y la palabra almacenamiento se usa para la memoria que existe en cintas o discos. Cada computadora viene con una cierta cantidad de memoria física, generalmente denominada memoria principal o RAM.

no heurístico

Este método de escaneo se basa en una base de datos de información de amenazas específicas. La ventaja del análisis no heurístico es que no se deja engañar por lo que podría parecer una amenaza y no genera falsas alarmas.

Depredadores en línea

Individuos que buscan atraer a menores o adolescentes a conversaciones con el propósito de involucrarlos en actividades sexuales ilegales. Las redes sociales son el lugar ideal donde los niños vulnerables pueden ser perseguidos y seducidos fácilmente para que cometan actividades sexuales, en línea o cara a cara.

Programas empaquetados

Un archivo en un formato de compresión. Muchos sistemas operativos y aplicaciones contienen comandos que le permiten empaquetar un archivo para que ocupe menos memoria. Por ejemplo, suponga que tiene un archivo de texto que contiene diez caracteres de espacio consecutivos. Normalmente, esto requeriría diez bytes de almacenamiento.

Sin embargo, un programa que empaqueta archivos reemplazaría los caracteres de espacio por un carácter de serie de espacio especial seguido por la cantidad de espacios que se reemplazan. En este caso, los diez espacios requerirían solo dos bytes. Esta es solo una técnica de empaque, hay muchas más.

Camino

Las direcciones exactas a un archivo en una computadora. Estas direcciones generalmente se describen mediante el sistema de archivo jerárquico de arriba hacia abajo.

La ruta entre dos puntos, como el canal de comunicación entre dos computadoras.

Suplantación de identidad

El acto de enviar un correo electrónico a un usuario que afirma falsamente ser una empresa legítima establecida en un intento de estafar al usuario para que entregue información privada que se utilizará para el robo de identidad. El correo electrónico dirige al usuario a visitar un sitio web donde se le pide que actualice la información personal, como contraseñas y números de tarjetas de crédito, seguridad social y cuentas bancarias, que ya tiene la organización legítima. El sitio web, sin embargo, es falso y está configurado solo para robar la información del usuario.

Fotón

Photon es una innovadora tecnología no intrusiva de Bitdefender, diseñada para minimizar el impacto en el rendimiento de su solución de seguridad. Al monitorear la actividad de su PC en segundo plano, crea patrones de uso que ayudan a optimizar los procesos de arranque y escaneo.

Virus polimórfico

Una amenaza que cambia de forma con cada archivo que infecta. Como no tienen un patrón binario constante, estas amenazas son difíciles de identificar.

Puerto

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

En las redes de tipo TCP/IP y UDP representa el endpoint 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.

Archivo de informe

Es un fichero que lista las acciones realizadas. BitDefender genera un archivo de informe (log) que contiene una lista de las rutas analizadas, las carpetas, el número de archivos y archivos comprimidos analizados, el número de archivos infectados y sospechosos que se han detectado.

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX y se refería a las herramientas que proporcionaban permisos de administrador a los intrusos, permitiéndoles ocultar su presencia para no ser vistos por los administradores de sistema.

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

Rootkits no son de naturaleza mala. Por ejemplo, los sistemas y algunas aplicaciones esconden ficheros críticos usando rootkits. No obstante, se usan habitualmente para ocultar amenazas o para encubrir la presencia

de un intruso en el sistema. Cuando se combinan con amenazas, los rootkits representan un gran peligro para la integridad y la seguridad de un sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar ficheros y logs y evitar su detección.

Script

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

Spam

Correo basura o posts basura en grupos de noticias. Se conoce generalmente como correo no deseado.

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 sobre direcciones de correo, e incluso contraseñas y números de tarjetas de crédito.

La similitud del spyware con una amenaza de tipo troyano radica en el hecho de que los usuarios instalan involuntariamente el producto al instalar otra cosa. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

Elementos de inicio

Todos los ficheros de esta carpeta se abren al iniciar el ordenador. Por ejemplo, una pantalla de inicio, un archivo de sonido para que se reproduzca cuando se inicie el equipo, un calendario de recordatorios o apps pueden ser elementos de inicio. Normalmente, se elige un alias del fichero para ubicar en esta carpeta y no directamente el fichero.

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.

Bandeja del sistema

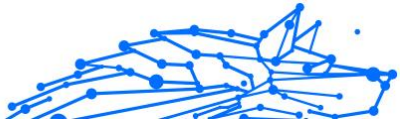
Elemento introducido con el sistema Windows 95,la bandeja de sistema está ubicada en la barra de tareas de Windows (normalmente al lado del reloj) y contiene iconos en miniatura para acceder fácilmente a las funciones del sistema, como el fax, la impresora, el módem, el volumen etc. Al hacer doble clic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

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.

Amenaza

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de las amenazas también pueden autorreplicarse. Todas las amenazas informáticas están creadas por el hombre. Una amenaza sencilla que pueda copiarse una y otra vez es relativamente fácil de producir. Incluso una amenaza tan simple es peligrosa porque consumirá rápidamente toda la memoria disponible y hará que el sistema se detenga. Un tipo de amenaza aún más peligrosa es la capaz de transmitirse a través de las redes y eludir los sistemas de seguridad.



Actualización de información sobre amenazas

El patrón binario de una amenaza, utilizado por la solución de seguridad para detectarla y eliminarla.

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los programas de software malicioso y gusanos, los troyanos no se autorreplican, pero pueden ser igualmente destructivos. Uno de los tipos de troyanos más graves es una amenaza que pretende desinfectar su equipo, pero en cambio introduce amenazas en él.

El término tiene origen en la famosa obra "La Ilíada" de Homero, en la cual Grecia entrega un gigantesco caballo de madera a sus enemigos, los Troyanos, como supuesta oferta de paz. Pero una vez los Troyanos arrastraron el caballo hasta el interior de las murallas de la ciudad, los soldados Griegos salieron de un hueco del vientre del caballo y abrieron las puertas de las murallas, permitiendo la entrada de sus compatriotas y la conquista de Troya.

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 posee una característica de actualización que le permite comprobar manualmente las actualizaciones o actualizar automáticamente el producto.

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.

Gusano

Un programa que se autopropaga a través de una red, reproduciéndose a medida que avanza. No puede adjuntarse a otros programas.