Bitdefender ANTIVIRUS PLUS

GUÍA DE USUARIO

Bitdefender Antivirus Plus
Guía de Usuario

fecha de publicación 12/09/2019

Advertencia legal

Bitdefender

Tabla de contenidos

PASOS DE LA INSTALACIÓN

1. PREPARÁNDOSE PARA LA INSTALACIÓN

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

- Asegúrese de que el equipo donde piensa instalar Bitdefender cumple los requisitos del sistema. Si el equipo 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*" (p. 3).
- Inicie sesión en el equipo utilizando una cuenta de Administrador.
- Desinstale cualquier otro software similar del equipo. 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.
- Durante la instalación, se recomienda que su equipo 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.

2. REQUISITOS DEL SISTEMA

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

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

- 2,5 GB de espacio disponible en disco duro (al menos 800 MB en la unidad de sistema)
- Intel CORE Duo (2 GHz) o procesador equivalente
- 2 GB de memoria (RAM)

Nota

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

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

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

2.1. Requisitos de software

Para poder usar Bitdefender y todas sus funciones, su equipo 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

3. INSTALANDO SU PRODUCTO BITDEFENDER

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

Si su compra cubre más de un equipo (por ejemplo, ha comprado Bitdefender Antivirus Plus para tres PC), repita el proceso de instalación y active su producto con la misma cuenta en cada equipo. La cuenta que tiene que utilizar es la que contiene la suscripción activa a su Bitdefender.

3.1. Instalar desde Bitdefender Central

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

Para descargar Bitdefender Antivirus Plus desde Bitdefender Central:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos** y, a continuación, haga clic en **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, a continuación, seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
     b. Haga clic en **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 comprobará primero su equipo 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 equipo para completar la eliminación de las soluciones de seguridad detectadas.

El paquete de instalación de Bitdefender Antivirus Plus está constantemente actualizado.

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

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

Paso 1 - Instalación de Bitdefender

Antes de proceder a la instalación, 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 Antivirus Plus.

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. Haga clic en **EMPEZAR A USAR Bitdefender** para continuar.

Paso 4 - 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 Antivirus Plus.

3.2. Instalar desde el disco de instalación

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

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

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

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

Validación de la instalación

Bitdefender comprobará primero su equipo para validar la instalación.

Si su sistema no cumple con los requisitos 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 equipo para completar la eliminación de las soluciones de seguridad detectadas.

Nota

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

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

Paso 1 - Instalación de Bitdefender

Antes de proceder a la instalación, 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 Antivirus Plus.

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

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. Haga clic en **EMPEZAR A USAR Bitdefender** para continuar.

Paso 4 - Cuenta Bitdefender

Tras completar la configuración inicial, aparece la ventana de Cuenta de Bitdefender. Es necesaria una cuenta Bitdefender para poder activar el producto y utilizar sus características online. Para más información, diríjase a "*Bitdefender Central*" (p. 32).

Proceder de acuerdo a su situación.

- **Quiero crear una cuenta 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 tengo 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 cuenta Bitdefender. Si ha olvidado su contraseña, primero tiene que ir a https://my.bitdefender.com para restablecerla. A continuación, utilice las credenciales actualizadas para iniciar sesión en cuenta Bitdefender.

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

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

1. Seleccione el servicio que desee usar. Será redirigido a la página de inicio de sesión de ese servicio.
2. Siga las instrucciones proporcionadas por el servicio seleccionado para vincular su cuenta a Bitdefender.

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

Paso 5 - Active su producto

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

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

Proceda de acuerdo con su situación:

- Tengo un código de activación

  En este caso, active el producto siguiendo estos pasos:

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

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

  2. **Deseo evaluar Bitdefender**

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

Paso 6 - 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 Antivirus Plus.

PRIMEROS PASOS

4. FUNDAMENTOS

Una vez que haya instalado Bitdefender Antivirus Plus, su equipo estará protegido contra todo tipo de amenazas (como malware, spyware, ransomware, exploits, botnets y troyanos).

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

La conexión a redes inalámbricas públicas pertenecientes a aeropuertos, centros comerciales, cafeterías u hoteles sin protección puede ser peligrosa para su dispositivo y sus datos. Ello se debe principalmente a que podría haber delincuentes vigilando sus actividades y esperando el mejor momento para robar sus datos personales, pero también a que cualquiera puede ver su dirección IP, lo que convierte a su equipo en víctima de futuros ataques informáticos. Para evitar situaciones tan comprometidas, instale y use la app "*VPN*" (p. 129).

Puede realizar un seguimiento de sus contraseñas y cuentas en Internet almacenándolas "*Protección del Gestor de contraseñas para sus credenciales*" (p. 118)en un wallet. Con una sola contraseña maestra, podrá proteger su privacidad frente a los intrusos que traten de arrebatarle su dinero.

Para protegerle ante posibles fisgones y espías cuando su dispositivo esté conectado a una red inalámbrica que no sea segura, Bitdefender analiza su nivel de seguridad y, si es necesario, le hace recomendaciones para aumentar la seguridad de sus actividades en Internet. Para obtener instrucciones sobre cómo mantener sus datos personales a salvo, consulte el apartado "*Asesor de seguridad Wi-Fi*" (p. 107).

Sus archivos personales almacenados localmente, como documentos, fotos o películas, y también los almacenados en la nube, pueden mantenerse a salvo de la amenaza más peligrosa a día de hoy: el ransomware. Para obtener información sobre cómo poner a buen recaudo sus archivos, consulte "*Archivos seguros*" (p. 112).

Los archivos cifrados por el ransomware se pueden recuperar ahora sin tener que pagar el dinero del rescate solicitado. Para obtener información sobre cómo recuperar los archivos cifrados, consulte "*Reparación de ransomware*" (p. 115).

Mientras trabaja, juega o ve películas, Bitdefender puede ofrecerle una experiencia de usuario constante posponiendo las tareas de mantenimiento, eliminando las interrupciones y ajustando los efectos visuales del sistema. Puede beneficiarse de todo esto activando y configurando los "*Perfiles*" (p. 143).

Bitdefender tomará por usted la mayoría de las decisiones relacionadas con la seguridad y rara vez se mostrarán alertas emergentes. Los detalles sobre las medidas adoptadas y la información acerca de la operativa del programa están disponibles en la ventana de Notificaciones. Para más información, diríjase a "*Notificaciones*" (p. 15).

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

Para usar las opciones online de Bitdefender Antivirus Plus y administrar sus suscripciones y dispositivos, acceda a su cuenta Bitdefender. Para más información, diríjase a "*Bitdefender Central*" (p. 32).

La sección "Cómo" (p. 45) es donde encontrará paso a paso instrucciones de cómo realizar tareas comunes. Si tiene algún problema mientras utiliza Bitdefender, revise la sección "*Resolución de incidencias comunes*" (p. 152) con soluciones para la mayoría de los problemas comunes.

4.1. Apertura de la ventana de Bitdefender

Para acceder a la interfaz principal de Bitdefender Antivirus Plus, siga estos pasos:

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

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

- En **Windows 10**:

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

Para obtener más información sobre la ventana de Bitdefender y el icono del área de notificación, consulte "*Interfaz de Bitdefender*" (p. 20).

4.2. Notificaciones

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

Las notificaciones son una herramienta importante en la supervisión y la gestión de la protección de Bitdefender. Por ejemplo, puede comprobar fácilmente si la actualización se realizó correctamente, si se encontraron vulnerabilidades o 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 comprobarlas y repararlas.
- Los eventos de **Información** indican operaciones que se han completado con éxito.

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

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

4.3. Perfiles

Algunas actividades informáticas, como los juegos online o las presentaciones en vídeo, requieren mayor capacidad de respuesta del sistema, alto rendimiento y ausencia de interrupciones. Cuando el portátil está funcionando con la batería, es mejor que las operaciones innecesarias, que consumen más energía, se aplacen hasta que el portátil está conectado de nuevo a la corriente.

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

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

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

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

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

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

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

4.3.1. Configurar la activación automática de perfiles

Para una experiencia de usuario sencilla, puede configurar Bitdefender para que gestione su perfil de trabajo. En tal caso, Bitdefender detecta

automáticamente la actividad que usted lleva a cabo y aplica los ajustes de optimización del producto y del sistema.

Para permitir que Bitdefender active los perfiles:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Utilice el conmutador correspondiente para habilitar **Activar perfiles automáticamente**.

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

Para activar manualmente un perfil, active el conmutador correspondiente. De los primeros tres perfiles, solo puede activarse manualmente uno a la vez.

Para obtener más información sobre los Perfiles, consulte"*Perfiles*" (p. 143)

4.4. Configuración de protección por contraseña de Bitdefender

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

Para configurar la protección por contraseña para los ajustes de Bitdefender:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. En la ventana **General**, active la **Protección por contraseña**.
3. Escriba la contraseña en los dos campos y haga clic en **Aceptar**. La contraseña debe tener al menos 8 caracteres.

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

Importante

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

Para eliminar protección por contraseña:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. En la ventana **General**, desactive la **Protección por contraseña**.
3. Escriba la contraseña y, a continuación, haga clic en **Aceptar**.

Nota

Para modificar la contraseña de su producto, haga clic en **Cambio de contraseña**. Escriba su contraseña actual y, a continuación, haga clic en **Aceptar**. En la ventana que aparece, escriba la nueva contraseña que desea utilizar a partir de ahora para restringir el acceso a sus ajustes de Bitdefender.

4.5. Informes de productos

Los informes del producto contienen información sobre cómo usa el producto Bitdefender que ha instalado. 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 utilizan con fines comerciales.

Si durante el proceso de instalación ha elegido enviar dichos informes a los servidores de Bitdefender y ahora desea detener dicho proceso:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Avanzado**.
3. Desactive los **Informes del producto**.

4.6. Notificaciones de 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. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. En la ventana **General**, active o desactive el conmutador correspondiente.

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

5. INTERFAZ DE BITDEFENDER

Bitdefender Antivirus Plus 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.

El icono de la bandeja del sistema de Bitdefender está disponible en cualquier momento, ya sea para abrir la ventana principal, ejecutar una actualización del producto o ver información sobre la versión instalada.

La ventana principal le brinda información sobre el estado de su seguridad. Según el uso y las necesidades de su dispositivo, Autopilot muestra aquí diferentes tipos de recomendaciones para ayudarle a mejorar la seguridad y el rendimiento de su dispositivo. Además, puede añadir las acciones rápidas que más use, para tenerlas a mano cuando las necesite.

Desde el menú de navegación de la izquierda, puede acceder a su cuenta de Bitdefender, al área de ajustes, a las notificaciones y a las secciones de Bitdefender para realizar una configuración detallada y tareas administrativas avanzadas. Además, puede ponerse en contacto con nosotros para obtener ayuda en caso de tener alguna pregunta o si sucede algo inesperado.

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

5.1. Icono del área de notificación

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

Nota

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

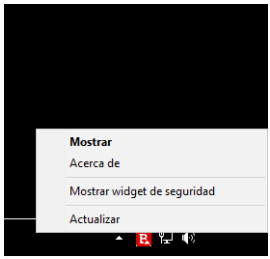
- En **Windows 7, Windows 8 y Windows 8.1**:
  1. Haga clic en la flecha en la esquina inferior derecha de la pantalla.

2. Haga clic en **Personalizar...** para abrir la ventana de Iconos del área de notificación.
3. Seleccione la opción **Mostrar icono y notificaciones** en el icono del **agente de Bitdefender**.

- En **Windows 10**:

1. Haga clic con el botón derecho en la barra de tareas y seleccione **Ajustes de la barra de tareas**.
2. Desplácese hacia abajo y haga clic en el enlace **Seleccionar qué iconos aparecen en la barra de tareas** en el **área de notificación**.
3. Active el conmutador junto al **agente de Bitdefender**.

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



Icono Bandeja

- **Mostrar** - abre la ventana principal de Bitdefender.
- **Acerca de**: Abre una ventana donde puede ver información sobre Bitdefender, buscar ayuda en caso de que suceda algo inesperado, acceder al Acuerdo de suscripción y ver los componentes de terceros y la política de privacidad.
- **Ocultar / Mostrar el Widget de seguridad** - habilita / deshabilita el Widget de seguridad.
- **Actualizar** - realiza una actualización inmediata. Puede seguir el estado de la actualización en el panel de Actualización de la ventana principal de Bitdefender.

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

No hay ninguna incidencia que afecte a la seguridad de su sistema.
Incidencias crítica afectan a la seguridad de su sistema. Requieren su atención inmediata y deben ser reparadas lo antes posible.

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

5.2. 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 y las herramientas 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 y realizar acciones rápidas.
- **Protección**. Desde aquí puede lanzar y configurar análisis antivirus, acceder a los ajustes del cortafuego, proteger archivos y apps de ataques de ransomware, recuperar datos en caso de que resulten cifrados por algún ransomware y configurar su protección mientras navega por Internet.
- **Privacidad**. Desde aquí puede crear gestores de contraseñas para sus cuentas online, proteger el acceso a su cámara web de miradas indiscretas, realizar pagos por Internet en un entorno seguro y abrir la app de VPN.
- **Notificaciones**. Desde aquí tiene acceso a las notificaciones generadas.
- **Mi cuenta**. Desde aquí puede acceder a su cuenta de Bitdefender para comprobar sus suscripciones y realizar tareas de seguridad en los dispositivos que administra. También dispone de información acerca de la cuenta de Bitdefender y de la suscripción en uso.
- **Ajustes**. Desde aquí tiene acceso a los ajustes generales.
- **Soporte**. Desde aquí, siempre que necesite ayuda para resolver cualquier incidencia con su Bitdefender Antivirus Plus, puede ponerse en contacto con el servicio de soporte técnico de Bitdefender.

5.3. Panel de Control

La ventana del panel de control le permite realizar tareas comunes, solucionar rápidamente problemas de seguridad, ver la información sobre el uso del producto y acceder a los paneles desde los cuales se configuran los ajustes.

Todo se encuentra a tan sólo unos clics.

La ventana está organizada en tres áreas principales:

Área de estado de seguridad
: Aquí es donde puede comprobar el estado de la seguridad de su equipo.

Autopilot
: Aquí es donde puede comprobar las recomendaciones de Autopilot para garantizar el adecuado funcionamiento del sistema.

Acciones rápidas
: Aquí es donde puede ejecutar diferentes tareas para mantener su sistema protegido.

5.3.1. Área de estado de seguridad

Bitdefender utiliza un sistema de seguimiento de incidencias para detectar e informarle sobre las incidencias que puedan afectar a la seguridad de su equipo e información. Las incidencias detectadas incluyen la desactivación de ajustes importantes de protección y otras condiciones que pueden representar un riesgo de seguridad.

Cuando existan problemas que afecten a la seguridad de su equipo, el estado que aparece en la parte superior de la interfaz de Bitdefender pasa a color rojo. El estado mostrado indica la naturaleza de los problemas que afectan a su sistema. Además, el icono de la bandeja del sistema cambia a y, si desplaza el cursor del ratón sobre el icono, una ventana emergente confirmará la existencia de problemas pendientes.

Dado que los problemas detectados pueden impedir que Bitdefender le proteja contra amenazas o suponga un gran riesgo para la seguridad, le recomendamos que preste atención y los solucione lo antes posible. Para solucionar un problema, haga clic en el botón junto al problema detectado.

5.3.2. Autopilot

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 (trabajo, pagos por Internet, ver películas o jugar) el Autopilot de Bitdefender le ofrecerá recomendaciones contextuales basadas en el uso y las necesidades de su dispositivo. Las recomendaciones propuestas también pueden estar relacionadas con las acciones que debe realizar para mantener su producto funcionando a la máxima capacidad.

Para comenzar a utilizar una característica sugerida o realizar mejoras en su producto, haga clic en el botón correspondiente.

Desactivar las notificaciones de Autopilot

Para llamar su atención respecto a las recomendaciones de Autopilot, el producto Bitdefender está configurado para realizar notificaciones mediante una ventana emergente.

Para desactivar las notificaciones de Autopilot:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. En la ventana **General**, desactive **Notificaciones de recomendación**.

5.3.3. Acciones rápidas

Mediante acciones rápidas, puede iniciar rápidamente tareas que considere importantes para mantener su sistema protegido y mejorar su forma de trabajar.

Por defecto, Bitdefender ya incorpora algunas acciones rápidas que puede sustituir por las que usted use más frecuentemente. Para reemplazar una acción rápida:

1. Haga clic en el icono + de la esquina superior derecha de la tarjeta que desee eliminar.
2. Escoja la tarea que desee añadir a la interfaz principal y, a continuación, haga clic en **AÑADIR**.

Las tareas que puede añadir a la interfaz principal son las siguientes:

- **Análisis rápido**. Ejecute un análisis rápido para detectar de inmediato las posibles amenazas que puedan existir en su equipo.
- **Análisis de sistema**. Ejecute un análisis del sistema para asegurarse de que su equipo está libre de amenazas.
- **Análisis de vulnerabilidades**. Analice su equipo en busca de vulnerabilidades para asegurarse de que todas las aplicaciones instaladas, además del sistema operativo, están actualizadas y funcionan correctamente.
- **Comprobar la seguridad de la conexión Wi-Fi**. Abra el Asesor de seguridad Wi-Fi para comprobar si la red doméstica inalámbrica a la que se conecta es segura y si tiene vulnerabilidades.

- **Wallets**. Ver y administrar sus wallets.
- **Abrir Safepay**. Abra Bitdefender Safepay™ para proteger sus datos confidenciales mientras efectúa transacciones online.
- **Abrir VPN**. Abra Bitdefender VPN para añadir una capa más de protección mientras permanece conectado a Internet.
- **Destructor de archivos**. Inicie la herramienta Destructor de archivos para eliminar todo rastro de datos confidenciales de su equipo.
-

Para empezar a proteger dispositivos adicionales con Bitdefender:

1. Haga clic en **Instalar en otro dispositivo**.

   Aparece una nueva ventana en la pantalla.

2. Haga clic en **COMPARTIR ENLACE DE DESCARGA**.

3. Siga los pasos que aparecen en la pantalla para instalar Bitdefender.

Dependiendo de su elección, se instalarán los siguientes productos de Bitdefender:

- Bitdefender Antivirus Plus en dispositivos basados ??en Windows.
- Bitdefender Antivirus for Mac en dispositivos basados ??en macOS.
- Bitdefender Mobile Security en dispositivos basados en Android.
- Bitdefender Mobile Security en dispositivos basados ??en iOS.

5.4. Las secciones de Bitdefender

El producto Bitdefender cuenta con dos secciones divididas en útiles características que le ayudarán a mantenerse protegido mientras trabaja, navega por la web, juega, o si desea efectuar pagos online.

Para acceder a las características de una determinada sección o para empezar a configurar su producto, acceda a los siguientes iconos situados en el menú de navegación de la interfaz de Bitdefender:

- Protección
- Privacidad

5.4.1. Protección

En la sección de Protección puede configurar sus ajustes de seguridad avanzados y las características de Archivos seguros y Prevención de amenazas online, buscar y corregir posibles vulnerabilidades del sistema y evaluar la seguridad de las redes inalámbricas a las que se conecta.

Las características que puede administrar en la sección de Protección son:

ANTIVIRUS

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

En la característica Antivirus puede acceder fácilmente a las siguientes tareas de análisis:

- Análisis rápido
- Análisis de sistema
- Administrar análisis
- Modo de Rescate (Entorno de rescate en Windows 10)

Si desea obtener más información sobre las tareas de análisis y sobre cómo configurar la protección antivirus, consulte "*Protección Antivirus*" (p. 75).

PREVENCIÓN DE AMENAZAS ONLINE

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

Para obtener más información sobre cómo configurar Bitdefender para proteger sus actividades en la Web, consulte "*Prevención de amenazas online*" (p. 100).

DEFENSA CONTRA AMENAZAS AVANZADAS

Advanced Threat Defense protege activamente su sistema contra amenazas como ransomware, spyware y troyanos, analizando el comportamiento de todas las apps instaladas. Se identifican los procesos sospechosos y, cuando es necesario, se bloquean.

Para obtener más información sobre cómo proteger su sistema contra amenazas, consulte "*Advanced Threat Defense*" (p. 97).

VULNERABILIDAD

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

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

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

Para obtener más información sobre la configuración de la protección contra vulnerabilidades, consulte "*Vulnerabilidad*" (p. 103).

ARCHIVOS SEGUROS

La característica de Archivos seguros le garantiza que sus archivos personales permanecerán protegidos contra los ataques de ransomware.

Para obtener más información sobre cómo configurar Archivos seguros para proteger sus archivos personales frente a los ataques de ransomware, consulte "*Archivos seguros*" (p. 112).

REPARACIÓN DE RANSOMWARE

La característica de Reparación de ransomware le ayuda a recuperar sus archivos en caso de que los cifre un ransomware.

Para obtener más información sobre cómo recuperar los archivos cifrados, consulte "*Reparación de ransomware*" (p. 115).

5.4.2. **Privacidad**

En la sección de Privacidad puede abrir la app Bitdefender VPN y proteger sus transacciones online y su experiencia de navegación.

Las características que puede administrar en la sección de Privacidad son:

VPN

Bitdefender VPN protege sus actividades online y oculta su dirección IP cada vez que se conecta a redes inalámbricas inseguras de aeropuertos,

centros comerciales, cafeterías u hoteles. Además, puede acceder a contenidos que normalmente le estarían vedados en ciertas zonas.

Para obtener más información sobre esta característica, consulte "*VPN*" (p. 129).

GESTOR DE CONTRASEÑAS

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

Para obtener más información sobre la configuración del Gestor de contraseñas, consulte "*Protección del Gestor de contraseñas para sus credenciales*" (p. 118).

SAFEPAY

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

Para obtener más información sobre Bitdefender Safepay™, consulte "*Seguridad Safepay para las transacciones online*" (p. 133).

PROTECCIÓN DE DATOS

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

Para obtener más información sobre la configuración de la Protección de datos, consulte "*Protección de datos*" (p. 139).

ANTI-TRACKER

Anti-tracker le ayuda a evitar que le rastreen, para preservar la privacidad de sus datos mientras navega por Internet, además de reducir el tiempo de carga de los sitios web.

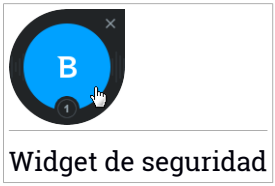
Para obtener más información sobre Anti-tracker, consulte "*Anti-tracker*" (p. 126).

5.5. Widget de seguridad

El **Widget de seguridad** es la forma rápida y fácil de monitorizar y controlar Bitdefender Antivirus Plus. Añadir este pequeño y no intrusivo widget a su

escritorio le permite ver la información crítica y realizar tareas clave en todo momento:

- abra la ventana principal de Bitdefender.
- monitorice la actividad del análisis en tiempo real.
- monitorice el estado de seguridad de su sistema y solucione cualquier incidencia existente.
- vea cuándo una actualización está en curso.
- vea las notificaciones y tenga acceso a los últimos eventos de los que haya informado Bitdefender.
- analice archivos o carpetas arrastrando y soltando uno o varios elementos sobre el widget.



Widget de seguridad

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

 Las incidencias críticas afectan a la seguridad de su sistema.

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

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

 Su sistema está protegido.

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

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

En la **parte inferior** del widget se muestra el contador de eventos no leídos (el número de eventos destacados de los que ha informado Bitdefender, si los hay). Haga clic en el contador de eventos, por ejemplo 1 para un evento no leído, para abrir la ventana de Notificaciones. Para más información, diríjase a "*Notificaciones*" (p. 15).

5.5.1. Análisis de archivos y carpetas

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

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

5.5.2. Ocultar / mostrar el Widget de seguridad

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

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

- Desde el área de notificación:
  1. Haga clic con el botón derecho en el icono de Bitdefender en la bandeja del sistema.
  2. Haga clic en **Mostrar widget de seguridad** en el menú contextual que aparece.
- Desde la interfaz de Bitdefender:
  1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
  2. En la ventana **General**, active el **Widget de seguridad**.

El widget de seguridad de Bitdefender está desactivado por defecto.

5.6. Cambiar el idioma del producto

La interfaz de Bitdefender está disponible en varios idiomas y se puede cambiar siguiendo estos pasos:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. En la ventana **General**, haga clic en **Cambiar idioma**.
3. Seleccione el idioma deseado de la lista y, a continuación, haga clic en **GUARDAR**.
4. Espere unos instantes a que se hayan aplicado los ajustes.

6. BITDEFENDER CENTRAL

Bitdefender Central es la plataforma en la que tiene acceso a los servicios y características online del producto y desde donde puede realizar de forma remota tareas importantes en los dispositivos en los que está instalado Bitdefender. Puede iniciar sesión en su cuenta de Bitdefender desde cualquier equipo conectado a Internet accediendo a https://central.bitdefender.com, o directamente desde la app Bitdefender Central en dispositivos Android e iOS.

Para instalar la app de Bitdefender Central en sus dispositivos:

- **En Android**: Busque Bitdefender Central en Google Play y luego descargue e instale la app. Siga los pasos necesarios para finalizar la instalación.
- **En iOS**: Busque Bitdefender Central en App Store y luego descargue e instale la app. Siga los pasos necesarios para finalizar la instalación.

Una vez que haya iniciado sesión, puede empezar por hacer lo siguiente:

- Descargue e instale Bitdefender en los sistemas operativos Windows, iOS, macOS y Android. Los productos disponibles para su descarga son:
  - Bitdefender Antivirus Plus
  - Bitdefender Antivirus for Mac
  - Bitdefender Mobile Security para Android
  - Bitdefender Mobile Security for iOS
- Administrar y renovar sus suscripciones de Bitdefender.
- Añadir nuevos dispositivos a su red y administrarlos desde cualquier lugar.

6.1. Acceso a Bitdefender Central

Existen varias formas de acceder Bitdefender Central:

- Desde la interfaz principal de Bitdefender:
  1. Haga clic en **Mi cuenta** en el menú de navegación de la interfaz de Bitdefender.
  2. Haga clic en **Acceder a Bitdefender Central**.
  3. Inicie sesión en su cuenta de Bitdefender con su dirección de correo electrónico y contraseña.

- Desde su navegador Web:
  1. Abra un navegador Web en cualquier dispositivo con acceso a internet.
  2. Diríjase a: https://central.bitdefender.com.
  3. Inicie sesión en su cuenta de Bitdefender con su dirección de correo electrónico y contraseña.
- Desde su dispositivo Android o iOS:

  Abra la app Bitdefender Central que ha instalado.

Nota
En este material, se le proporcionan las opciones e instrucciones disponibles en la plataforma web.

6.2. Autenticación en dos fases

El método de autenticación en dos fases aporta una capa adicional de seguridad a su cuenta de Bitdefender, ya que requiere un código de autenticación además de sus credenciales de inicio de sesión. De esta manera, evitará la toma de control de la cuenta y mantendrá alejados ciertos tipos de ataques informáticos, como los de registradores de pulsaciones de teclas, los de fuerza bruta o los de diccionario.

Activar la autenticación en dos fases

Al habilitar la autenticación en dos fases, su cuenta de Bitdefender estará mucho más segura. Su identidad se verificará cada vez que inicie sesión desde diferentes dispositivos, ya sea para instalar uno de los productos de Bitdefender, para verificar el estado de su suscripción o para ejecutar tareas en sus dispositivos de forma remota.

Para habilitar la autenticación en dos fases:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono de la parte superior derecha de la pantalla.
3. Haga clic en **Cuenta de Bitdefender** en el menú deslizante.
4. Seleccione la pestaña **Contraseña y seguridad**.
5. Haga clic en **Autenticación en dos fases**.
6. Haga clic en **PUESTA EN MARCHA**.

Escoja uno de los siguientes métodos:

- **App de autenticación**: Use una app de autenticación para generar un código cada vez que desee iniciar sesión en su cuenta de Bitdefender.

  Si desea utilizar una app de autenticación, pero no está seguro de cuál elegir, tiene a su disposición una lista con las que recomendamos.

  a. Haga clic en **USAR LA APP DE AUTENTICACIÓN** para comenzar.

  b. Para iniciar sesión en un dispositivo con Android o iOS, use su dispositivo para leer el código QR.

  Para iniciar sesión en un equipo de escritorio o portátil, puede añadir manualmente el código mostrado.

  Haga clic en **CONTINUAR**.

  c. Inserte el código proporcionado por la app o el que se muestra en el paso anterior y, a continuación, haga clic en **ACTIVAR**.

- **Correo electrónico**: Cada vez que inicie sesión en su cuenta de Bitdefender, se le enviará un código de verificación a su bandeja de entrada de correo electrónico. Consulte su cuenta de correo electrónico e introduzca el código que reciba.

  a. Haga clic en **USAR CORREO ELECTRÓNICO** para comenzar.

  b. Consulte su cuenta de correo electrónico y escriba el código que se le proporciona.

  Tenga en cuenta que tiene cinco minutos para revisar su cuenta de correo electrónico y escribir el código generado. Si se agotase el tiempo, debería generar uno nuevo siguiendo los mismos pasos.

  c. Haga clic en **ACTIVAR**.

  d. Se le proporcionan diez códigos de activación. Puede copiar, descargar o imprimir la lista y utilizarla en caso de que pierda su dirección de correo electrónico o no pueda iniciar sesión. Los códigos solo se pueden usar una vez.

  e. Haga clic en **HECHO**.

En caso de que desee dejar de usar la autenticación en dos fases:

1. Haga clic en **DESACTIVAR LA AUTENTICACIÓN EN DOS FASES**.
2. Consulte su app o su cuenta de correo electrónico y escriba el código que ha recibido.

En caso de que haya optado por recibir el código de autenticación por correo electrónico, tiene cinco minutos para consultar su cuenta de correo electrónico y escribir el código generado. Si se agotase el tiempo, debería generar uno nuevo siguiendo los mismos pasos.

3. Confirme su elección.

6.2.1. Añadir dispositivos de confianza

Para asegurarnos de que solo usted pueda acceder a su cuenta de Bitdefender, es posible que le solicitemos antes un código de seguridad. Si desea omitir este paso siempre que se conecte desde el mismo dispositivo, le recomendamos que lo añada como dispositivo de confianza.

Para añadir dispositivos de confianza:

1. Acceda a Bitdefender Central.
2. Haga clic en el icono de la parte superior derecha de la pantalla.
3. Haga clic en **Cuenta de Bitdefender** en el menú deslizante.
4. Seleccione la pestaña **Contraseña y seguridad**.
5. Haga clic en **Dispositivos de confianza**.
6. Aparecerá la lista con los dispositivos en los que está instalado Bitdefender. Haga clic en el dispositivo deseado.

Puede añadir tantos dispositivos como desee, siempre y cuando tengan Bitdefender instalado y su suscripción sea válida.

6.3. Mis suscripciones

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

6.3.1. Compruebe las suscripciones disponibles

Para comprobar sus suscripciones disponibles:

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

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

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

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

6.3.2. Añadir un nuevo dispositivo

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

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos** y, a continuación, haga clic en **INSTALAR PROTECCIÓN**.
3. Escoja una de las dos opciones disponibles:
   - **Proteger este dispositivo**

     Seleccione esta opción y, a continuación, 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, a continuación, seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.

     Haga clic en **ENVIAR ENLACE DE DESCARGA**. 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.

     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.

6.3.3. Renovar la suscripción

Si ha inhabilitado la renovación automática de su suscripción de Bitdefender, puede renovarla manualmente siguiendo los pasos que se exponen a continuación:

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

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

6.3.4. Activar la suscripción

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

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

Para activar una suscripción mediante un código de activación:

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

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

6.4. Mis dispositivos

El área **Mis dispositivos** en Bitdefender Central le da la posibilidad de instalar, administrar y llevar a cabo acciones remotas en su producto de Bitdefender en cualquier dispositivo, siempre y cuando esté encendido y conectado a

internet. Las tarjetas de cada dispositivo muestran el nombre de este, su estado de protección y si existen riesgos para la seguridad que afecten a la protección de sus dispositivos.

Para ver una lista de sus dispositivos ordenados según su estado o usuarios, haga clic en la flecha desplegable de la esquina superior derecha de la pantalla.

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

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en la tarjeta del dispositivo deseado y, a continuación, en el icono ⋮ de la esquina superior derecha de la pantalla.
4. Seleccione **Ajustes**.
5. Escriba un nuevo nombre en el campo **Nombre del dispositivo** y, a continuación, haga clic en **GUARDAR**.

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

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en la tarjeta del dispositivo deseado y, a continuación, en el icono ⋮ de la esquina superior derecha de la pantalla.
4. Seleccione **Perfil**.
5. Haga clic en **Añadir propietario** y, a continuación, rellene los campos correspondientes. Personalice el perfil añadiendo una foto y seleccionando una fecha de nacimiento.
6. Haga clic en **AÑADIR** para guardar el perfil.
7. Seleccione el propietario deseado en la lista de **Propietarios de dispositivos** y, a continuación, haga clic en **ASIGNAR**.

Para actualizar Bitdefender en un dispositivo Windows:

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

3. Haga clic en la tarjeta del dispositivo deseado y, a continuación, en el icono ⋮ de la esquina superior derecha de la pantalla.
4. Seleccione **Actualización**.

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

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

- **Panel de Control**. En esta ventana puede ver información sobre el dispositivo seleccionado, comprobar el estado de su protección, el de Bitdefender VPN y cuántas amenazas se han bloqueado en los últimos siete días. El estado de la protección puede ser verde, cuando no hay ningún problema que afecte a su producto; amarillo, si el dispositivo requiere su atención; o rojo, cuando el dispositivo está en riesgo. Cuando haya problemas que afecten a su dispositivo, haga clic en la flecha desplegable en el área de estado superior para obtener más información. Desde aquí puede solucionar manualmente las incidencias que estén afectando a la seguridad de sus dispositivos.
- **Protección**. Desde esta ventana puede ejecutar de forma remota un análisis rápido o un análisis del sistema en sus dispositivos. Haga clic en el botón **ANALIZAR** para poner en marcha el proceso. También puede comprobar cuándo se realizó el último análisis en el dispositivo, así como obtener un informe del último análisis con la información más importante disponible.Para más información sobre estos dos procesos de análisis, consulte "*Ejecución de un análisis del sistema*" (p. 82) y "*Ejecución de un análisis Quick Scan*" (p. 82).
- **Vulnerabilidad**. Para comprobar las vulnerabilidades de un dispositivo, como por ejemplo actualizaciones de Windows sin hacer, aplicaciones obsoletas o contraseñas débiles, haga clic en el botón **ANALIZAR** en la pestaña de Vulnerabilidad. Las vulnerabilidades no se pueden solucionar de forma remota. En caso de encontrar cualquier vulnerabilidad, tendrá que ejecutar un nuevo análisis en el dispositivo y adoptar las medidas recomendadas. Haga clic en **Más detalles** para acceder a un informe detallado acerca de los problemas encontrados. Para más información sobre esta característica, consulte "*Vulnerabilidad*" (p. 103).

6.5. Notificaciones

Para ayudarle a mantenerse informado de lo que sucede en los dispositivos asociados a su cuenta, tiene fácilmente accesible el icono 🔔. Haciendo clic en él dispondrá de una panorámica general con información acerca de la actividad de los productos de Bitdefender instalados en sus dispositivos.

7. MANTENIMIENTO DE BITDEFENDER AL DÍA

Todos los días se encuentran e identifican nuevas amenazas. Por este motivo es muy importante mantener Bitdefender actualizado con la última base de datos de información de amenazas.

Si está conectado a internet a través de una conexión de banda ancha o ADSL, Bitdefender se actualizará sólo. Por omisión, busca actualizaciones cuando enciende su equipo y cada **hora** a partir de ese momento. Si se detecta una actualización, esta es automáticamente descargada e instalada en su equipo.

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

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

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

- Si su equipo se conecta a internet a través de un servidor proxy, puede configurar las opciones del proxy según se describe en "*¿Cómo configuro Bitdefender para usar una conexión a Internet mediante proxy?*" (p. 68).
- Si está conectado a internet a través de una conexión por módem analógico, es recomendable actualizar Bitdefender manualmente. Para más información, diríjase a "*Realizar una actualización*" (p. 42).

7.1. Comprobar si Bitdefender está actualizado

Para comprobar la hora a la que se actualizó su Bitdefender por última vez:

1. Haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente a la última actualización.

Puede saber cuándo se iniciaron las actualizaciones y obtener información sobre ellas (si se realizaron con éxito o no, si requieren reiniciar para

completar la instalación). Si es necesario, reinicie el sistema en cuanto pueda.

7.2. Realizar una actualización

Para poder hacer actualizaciones es necesaria una conexión a internet.

Para comenzar una actualización, haga clic con el botón derecho en el icono de Bitdefender en la bandeja del sistema y, a continuación, seleccione **Actualizar ahora**.

La característica Actualizar se conectará al Servidor de actualizaciones de Bitdefender y buscará actualizaciones. Al detectar una actualización se le solicitará su confirmación para instalarla, o bien podrá realizarse de forma automática dependiendo de lo haya definido en la Configuración de actualización.

Importante
Podría ser necesario reiniciar el equipo cuando haya completado la actualización. Le recomendamos que lo haga lo antes posible.

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

Para actualizar Bitdefender en un dispositivo Windows:

1. Acceda a Bitdefender Central.
2. Seleccione el panel **Mis dispositivos**.
3. Haga clic en la tarjeta del dispositivo deseado y, a continuación, en el icono de la esquina superior derecha de la pantalla.
4. Seleccione **Actualización**.

7.3. Activar o desactivar la actualización automática

Para activar o desactivar la actualización automática:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Actualizar**.
3. Active o desactive el conmutador correspondiente.

4. Aparecerá una ventana de advertencia. Debe confirmar esta elección seleccionando del menú cuánto tiempo desea que esté deshabilitada la actualización automática. Puede desactivar la actualización automática durante cinco, quince o treinta minutos, una hora o hasta que se reinicie el sistema.

Aviso
Se trata de una cuestión crítica para la seguridad de su sistema. Recomendamos desactivar la protección en tiempo real durante el menor tiempo posible. Si Bitdefender no se actualiza regularmente, no podrá protegerle contra las amenazas más recientes.

7.4. Ajustar las opciones de actualización

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

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

Para modificar los ajustes de actualización:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Actualizar** y ajuste la configuración de acuerdo a sus preferencias.

Frecuencia de actualización

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

Reglas de proceso de actualización

Siempre que haya una actualización disponible, Bitdefender descargará e implementará automáticamente la actualización sin mostrar notificaciones. Desactive la opción **Actualización silenciosa** si desea que se le notifique cada vez que haya una nueva actualización disponible.

Algunas actualizaciones necesitan reiniciar el sistema para completar la instalación.

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

Si desea que se le pregunte cuando una actualización requiera reiniciar, active **Notificación de reinicio**.

7.5. Actualizaciones continuas

Para asegurarse de que está utilizando la última versión, su Bitdefender comprueba automáticamente si existen actualizaciones del producto. Estas actualizaciones pueden aportar nuevas características y mejoras, solucionar problemas del producto o actualizarlo automáticamente a una nueva versión. Cuando se produce una actualización a una nueva versión de Bitdefender, se guardan los ajustes personalizados y se omite el proceso de desinstalación y reinstalación.

Estas actualizaciones requieren un reinicio del sistema para dar paso a la instalación de nuevos archivos. Cuando se complete una actualización del producto, una ventana emergente le informará de que debe reiniciar el sistema. Si pasa por alto esta notificación, puede hacer clic en **REINICIAR AHORA** en la ventana Notificaciones donde se indica la actualización más reciente, o reiniciar manualmente el sistema.

Nota
Las actualizaciones que incluyan nuevas características y mejoras se proporcionarán únicamente a los usuarios que tengan Bitdefender 2019 instalado.

CÓMO

8. PASOS DE LA INSTALACIÓN

8.1. ¿Cómo instalo Bitdefender en un segundo equipo?

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

Para instalar Bitdefender en un segundo equipo:

1. Haga clic en **Instalar en otro dispositivo** en la esquina inferior izquierda de la interfaz de Bitdefender.

   Aparece una nueva ventana en la pantalla.

2. Haga clic en **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.

8.2. ¿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.

Si experimenta alguna de las situaciones mencionadas, siga estos pasos:

- En **Windows 7**:
  1. Haga clic en **Inicio** y diríjase a **Todos los programas**.
  2. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
  3. Haga clic en **REINSTALAR** en la ventana que aparece.
  4. Necesita reiniciar el equipo para completar el proceso.
- En **Windows 8 y Windows 8.1**:

1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
2. Haga clic en **Desinstalar un programa** o **Programas y características**.
3. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
4. Haga clic en **REINSTALAR** en la ventana que aparece.
5. Necesita reiniciar el equipo para completar el proceso.

- En **Windows 10**:

1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Apps y características**.
3. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
4. Haga clic en **Desinstalar** para confirmar su elección.
5. Haga clic en **REINSTALAR**.
6. Necesita reiniciar el equipo 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.

8.3. ¿Desde dónde puedo descargar mi producto Bitdefender?

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

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

Para instalar Bitdefender desde Bitdefender Central:

1. Acceda a Bitdefender Central.

2. Seleccione el panel **Mis dispositivos** y, a continuación, haga clic en **INSTALAR PROTECCIÓN**.
3. Escoja una de las dos opciones disponibles:

   - **Proteger este dispositivo**

     Seleccione esta opción y, a continuación, 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, a continuación, seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.

     Haga clic en **ENVIAR ENLACE DE DESCARGA**. 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.

     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. Ejecute el producto Bitdefender que ha descargado.

8.4. ¿Cómo puedo cambiar el idioma de mi producto Bitdefender?

La interfaz de Bitdefender está disponible en varios idiomas y se puede cambiar siguiendo estos pasos:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. En la ventana **General**, haga clic en **Cambiar idioma**.
3. Seleccione el idioma deseado de la lista y, a continuación, haga clic en **GUARDAR**.
4. Espere unos instantes a que se hayan aplicado los ajustes.

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

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

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

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

Existen 2 casos que pueden aparecer:

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

  En este caso, necesita reinstalar el producto siguiendo estos pasos:

  - En **Windows 7**:

    1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
    2. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
    3. Haga clic en **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 **Windows 8 y Windows 8.1**:

    1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
    2. Haga clic en **Desinstalar un programa** o **Programas y características**.
    3. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.

4. Haga clic en **REINSTALAR** en la ventana que aparece.
5. 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 **Windows 10**:

1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones**.
3. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
4. Haga clic en **Desinstalar** para confirmar su elección.
5. Haga clic en **REINSTALAR** en la ventana que aparece.
6. 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.

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.

- Ha cambiado su sistema y desea seguir utilizando la protección de Bitdefender. Por tanto, necesitará reinstalar el producto utilizando la última versión.

  Para resolver esta situación:

1. Descargue el archivo de instalación:
   a. Acceda a Bitdefender Central.
   b. Seleccione el panel **Mis dispositivos** y, a continuación, haga clic en **INSTALAR PROTECCIÓN**.
   c. Escoja una de las dos opciones disponibles:
      - **Proteger este dispositivo**

Seleccione esta opción y, a continuación, 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, a continuación, seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.

  Haga clic en **ENVIAR ENLACE DE DESCARGA**. 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.

  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.

2. Ejecute el producto Bitdefender que ha descargado.

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

8.6. ¿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 2019, 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 equipo.

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.

9. BITDEFENDER CENTRAL

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

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

Para poder iniciar sesión con otra cuenta de Bitdefender:

1. Haga clic en **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 para cambiar la cuenta vinculada al equipo.
3. Escriba la dirección de correo electrónico en el campo correspondiente y, a continuación, haga clic en **SIGUIENTE**.
4. Escriba su contraseña y, a continuación, haga clic en **INICIAR SESIÓN**.

Nota
El producto Bitdefender de su dispositivo cambia automáticamente de acuerdo con la suscripción asociada a la nueva cuenta de Bitdefender.
Si no hay ninguna suscripción disponible asociada a la nueva cuenta de Bitdefender, o si desea transferirla desde la cuenta anterior, puede ponerse en contacto con el soporte técnico de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 176).

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

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

Si no desea ver este tipo de mensajes:

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

9.3. 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 la interfaz de Bitdefender:
  1. Haga clic en **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. Haga clic en **¿Olvidó la contraseña?**.
  4. Escriba su cuenta de correo electrónico y haga clic en **SIGUIENTE**.
  5. 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.
  6. Escriba la nueva contraseña que desea establecer y, luego, vuelva a escribirla. Haga clic en **GUARDAR**.
- Desde su navegador Web:
  1. Diríjase a: https://central.bitdefender.com.
  2. Haga clic en **INICIAR SESIÓN**.
  3. Escriba su dirección de correo electrónico y, a continuación, haga clic en **SIGUIENTE**.
  4. Haga clic en **¿Olvidó la contraseña?**.
  5. 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.

9.4. ¿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. Acceda a Bitdefender Central.
2. Haga clic en el icono de la parte superior derecha de la pantalla.
3. Haga clic en **Mi cuenta** en el menú deslizante.
4. Haga clic en **Gestión de sesiones** en el menú deslizante.
5. En la sección **Sesiones activas**, seleccione la opción **CERRAR SESIÓN** junto al dispositivo en el que desee cerrar la sesión.

10. ANALIZANDO CON BITDEFENDER

10.1. ¿Cómo analizo un archivo o una carpeta?

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

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

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

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

- Sospecha que un fichero o carpeta concreta está infectada.
- Siempre que descargue archivos de internet que crea que pueden ser peligrosos.
- Analizar una carpeta compartida en red antes de copiar ficheros a su ordenador.

10.2. ¿Cómo analizo mi sistema?

Para llevar a cabo un análisis completo del sistema:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Análisis del sistema**.
3. 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 "*Asistente del análisis Antivirus*" (p. 86).

10.3. ¿Cómo puedo programar un análisis?

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

Para programar un análisis:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Administrar análisis**.
3. Haga clic en junto al tipo de análisis que desea programar: Análisis del sistema o Quick Scan.

   Como alternativa, puede crear un tipo de análisis que se adapte a sus necesidades haciendo clic en **Crear una nueva tarea de análisis**.
4. Active la opción **Programar tarea de análisis**.

   Seleccione una de las opciones correspondientes para establecer una programación:

   - Al iniciar el sistema
   - Diariamente
   - Semanalmente
   - Mensualmente

   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.

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.

10.4. ¿Cómo creo una tarea de análisis personalizada?

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

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

1. En el panel **ANTIVIRUS**, haga clic en **Administrar análisis**.

2. Haga clic en **Crear una nueva tarea de análisis**.
3. 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**.
4. Configure estas opciones generales:
   - **Analizar únicamente aplicaciones**. Puede configurar Bitdefender para analizar solo las apps 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 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
5. Si desea configurar detalladamente las opciones de análisis, haga clic en **Mostrar opciones avanzadas**.

   Haga clic en **SIGUIENTE**.
6. Habilite **Programar tarea de análisis** y, a continuación, elija 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.

7. 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.

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

10.5. ¿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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. Haga clic en la pestaña **Excepciones**.
4. Haga clic en el menú de acordeón **Lista de archivos y carpetas exceptuados del análisis** y, a continuación, en el botón **Añadir**.

5. Haga clic en **EXAMINAR**, seleccione la carpeta que desea exceptuar del análisis y, a continuación, elija el tipo de análisis del que se debe exceptuar.
6. Haga clic en **AÑADIR** para aplicar los cambios y cierre la ventana.

10.6. ¿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. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
   b. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
   c. En la ventana **Escudo**, desactive **Escudo de Bitdefender**.

      Aparecerá una ventana de advertencia. Debe confirmar su elección seleccionando en el menú cuanto tiempo desea que la protección en tiempo real esté desactivada. Puede desactivar la protección en tiempo real durante cinco, quince o treinta minutos, durante una hora, de forma permanente o hasta que se reinicie el sistema.
2. Muestra los objetos ocultos en Windows. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo mostrar los objetos ocultos en Windows?*" (p. 70).
3. Restaurar el archivo desde el área de Cuarentena:
   a. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
   b. En el panel **ANTIVIRUS**, haga clic en **Cuarentena**.
   c. Seleccione el archivo y 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?*" (p. 59).
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 "*Pedir ayuda*" (p. 176).

10.7. ¿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 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. Haga clic en **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 un registro de análisis, haga clic en **Ver log**.

11. PROTECCIÓN DE PRIVACIDAD

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

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

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

Para mantener sus actividades online protegidas y en privado:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **SAFEPAY**, haga clic en **Abrir Safepay**.
3. Haga clic en el botón  para acceder al **Teclado virtual**.

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

11.2. ¿Cómo elimino permanentemente un archivo con Bitdefender?

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

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

1. Haga clic con el botón derecho en el archivo o carpeta que desee eliminar permanentemente, escoja Bitdefender y seleccione **Destructor de archivos**.
2. Haga clic en **ELIMINAR PERMANENTEMENTE** y, a continuación, confirme que desea continuar con el proceso.

   Espere a que Bitdefender finalice la destrucción de archivos.

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

11.3. ¿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. Haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación referente al 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;

12. INFORMACIÓN DE UTILIDAD

12.1. ¿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 "*Pedir ayuda*" (p. 176).

12.2. ¿Cómo puedo eliminar Bitdefender?

Si desea eliminar su Bitdefender Antivirus Plus:

- En **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
  3. Haga clic en **ELIMINAR** en la ventana que aparece.

4. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

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

1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
2. Haga clic en **Desinstalar un programa** o **Programas y características**.
3. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
4. Haga clic en **ELIMINAR** en la ventana que aparece.
5. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

- En **Windows 10**:

1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones**.
3. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
4. Haga clic en **Desinstalar** para confirmar su elección.
5. Haga clic en **ELIMINAR** en la ventana que aparece.
6. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

Nota
Este procedimiento de reinstalación eliminará permanentemente los ajustes personalizados.

12.3. ¿Cómo puedo eliminar Bitdefender VPN?

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

- En **Windows 7**:

1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
2. Encuentre **Bitdefender VPN** 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. Encuentre **Bitdefender VPN** y seleccione **Desinstalar**.

     Espere a que el proceso de desinstalación se complete.
- En **Windows 10**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
  3. Encuentre **Bitdefender VPN** y seleccione **Desinstalar**.
  4. Haga clic en **Desinstalar** para confirmar su elección.

     Espere a que el proceso de desinstalación se complete.

12.4. ¿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:

- Internet Explorer
  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. Haga clic en  junto a la barra de búsqueda.
2. Seleccione **Complementos** y, a continuación, **Extensiones**.

   Se mostrará una lista con las extensiones instaladas.
3. Haga clic en **Eliminar** en la tarjeta de Bitdefender Anti-tracker.

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

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

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

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

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

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Administrar análisis**.
3. Haga clic en  junto a Quick Scan o a Análisis del sistema.
4. En la lista de **Acciones posteriores al análisis**, seleccione **Apagar el dispositivo** y, a continuación, haga clic en **SIGUIENTE**.
5. Habilite **Programar tarea de análisis** y, a continuación, elija cuándo debe iniciarse la tarea.

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.

Para apagar el equipo al finalizar un análisis personalizado:

1. Haga clic en junto al análisis personalizado que ha creado.
2. En la ventana **Tarea de análisis**, haga clic en **SIGUIENTE**.
3. En la lista de **Acciones posteriores al análisis**, seleccione **Apagar el dispositivo**.
4. Haga clic en **SIGUIENTE** y, a continuación, haga clic en **GUARDAR**.

Si no se encuentran amenazas, su equipo se apagará.

Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas. Para más información, diríjase a "*Asistente del análisis Antivirus*" (p. 86).

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

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

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

Para administrar las opciones del proxy:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Avanzado**.
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 IP del servidor proxy.
     - **Puerto** - introduzca el puerto que Bitdefender debe utilizar para conectarse con el servidor proxy.
     - **Nombre** - escriba un nombre de usuario que el proxy reconozca.
     - **Contraseña** - escriba una contraseña válida para el usuario indicado anteriormente.
6. Haga clic en **Aceptar** para guardar los cambios y cerrar la ventana.

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

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

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

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

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

   En **Windows 8.1**, acceda a **Este equipo**.

2. Seleccione **Propiedades** en el menú inferior.
3. Consulte el área del sistema para ver su tipo de sistema.

- En **Windows 10**:

1. Escriba "Sistema" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono.
2. Consulte el área del sistema para obtener información sobre el tipo de sistema.

12.8. ¿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 **Inicio**, y vaya al **Panel de control**.

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

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

En **Windows 10**:

1. Escriba "Mostrar todos los archivos y carpetas ocultos" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono.

2. Seleccione **Mostrar archivos, carpetas y unidades ocultos**.
3. Desmarcar **Ocultar extensiones para tipos de archivo conocidos**.
4. Desmarque **Ocultar archivos protegidos del sistema operativo**.
5. Haga clic en **Aplicar** y, a continuación, haga clic en **Aceptar**.

12.9. ¿Cómo desinstalo otras soluciones de seguridad?

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

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

Si no desea eliminar las otras soluciones de seguridad durante la instalación inicial:

- En **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Espere un momento a que el software instalado se muestre.
  3. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  4. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Desinstalar un programa** o **Programas y características**.
  3. Espere un momento a que el software instalado se muestre.
  4. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.

5. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

- En **Windows 10**:

1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones**.
3. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
4. Haga clic en **Desinstalar** para confirmar su elección.
5. Espere a que finalice 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.

12.10. ¿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 **Windows 7**:

1. Reinicie el equipo.
2. Presione la tecla **F8** varias veces antes de iniciar Windows para tener acceso al menú de inicio.
3. Seleccione **Modo seguro** en el menú de arranque o **Modo seguro con red** si quiere disponer de acceso a internet.
4. Presione la tecla **Intro** y espere mientras Windows se carga en Modo seguro.

5. Este proceso finaliza con un mensaje de confirmación. Haga clic en **OK** para reconocer.
6. Para iniciar Windows normal, simplemente reinicie el sistema.

- En **Windows 8, Windows 8.1 y Windows 10**:

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

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

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

GESTIÓN DE SU SEGURIDAD

13. PROTECCIÓN ANTIVIRUS

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

- 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 equipo, 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 equipo para así asegurarse de que se puede acceder al mismo de forma segura. Para más información, diríjase a "*Análisis automático de los medios extraíbles*" (p. 90).

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*" (p. 93).

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*" (p. 95).

Si su equipo se ha visto infectado con amenazas, consulte "*Eliminación de amenazas de su sistema*" (p. 165). Para ayudarle a limpiar su equipo de amenazas que no pueden eliminarse desde el propio sistema operativo Windows, Bitdefender le ofrece"*Bitdefender Modo de Rescate (Entorno de*

rescate en Windows 10)" (p. 165). Este es un entorno de confianza, especialmente diseñado para la eliminación de amenazas, lo que le permite arrancar el equipo independientemente de Windows. Cuando el equipo se ejecuta en modo Rescate (Entorno de rescate en Windows 10), las amenazas de Windows están inactivas, por lo que es fácil eliminarlas.

13.1. 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.

13.1.1. 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 **Ajustes**.
3. En la ventana **Escudo**, active o desactive **Escudo de Bitdefender**.
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.

Aviso
Se trata de una cuestión crítica para la seguridad de su sistema. Recomendamos desactivar la protección en tiempo real durante el menor tiempo posible. Si desactiva la protección en tiempo real, no estará protegido contra las amenazas.

13.1.2. 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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. En la ventana **Escudo**, haga clic en el menú de acordeón **Mostrar ajustes avanzados**.

   Se muestra una ventana con paneles.
4. Desplácese hacia abajo por la ventana para configurar los ajustes de análisis según sea preciso.

Información sobre las opciones de análisis

Puede que esta información le sea útil:

- **Analizar únicamente aplicaciones.** Puede configurar Bitdefender para analizar solo las apps a las que accede.
- **Analizar en busca de aplicaciones potencialmente no deseadas.** Seleccione esta opción para analizar en busca de 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 equipo, le recomendamos que mantenga habilitada la opción Analizar recursos compartidos.
- **Analizar archivos comprimidos.** Analizar dentro de archivos es una proceso lento, requiere muchos recursos, por esta razón no lo recomendamos para

la protección en tiempo real. Los archivos que contienen archivos infectados no son amenazas inmediatas para la seguridad de sus sistema. 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 emails.** Para evitar que se descarguen amenazas en su equipo, Bitdefender analiza automáticamente los mensajes de correo electrónico entrantes y salientes.

  Aunque no es recomendable, puede desactivar el análisis de amenazas del correo electrónico para mejorar el rendimiento de su sistema. Si desactiva las opciones de análisis correspondientes, no se analizarán los mensajes de correo electrónico y sus posibles adjuntos, lo que permitirá que los archivos infectados se guarden en su equipo. Esta no es una amenaza importante porque la protección en tiempo real bloqueará la amenaza cuando se acceda a los archivos infectados (se abran, muevan, copien o ejecuten).

- **Analizar los sectores de arranque.** Puede configurar Bitdefender para que analice los sectores de arranque de su disco duro. Este sector del disco duro contiene el código del equipo necesario para iniciar el proceso de arranque. Cuando una amenaza infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar sus 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 keyloggers.** Seleccione esta opción para analizar su sistema en busca de aplicaciones keylogger. Los Keyloggers registran lo que escribe en el teclado y envían informes por internet a alguien con malas intenciones (hacker). El hacker puede encontrar información personal entre los datos robados, como números de cuentas bancarias o contraseñas, pudiendo utilizarlos para su propio beneficio.

- **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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. En la ventana **Escudo**, haga clic en el menú de acordeón **Mostrar ajustes avanzados**.

   Se muestra una ventana con paneles.
4. Desplácese hacia abajo por la ventana hasta que aparezca la opción **Acciones de amenazas**.
5. Configure los ajustes del análisis como necesite.

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

Adoptar medidas

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

- **Archivos infectados.** Los archivos detectados como infectados coinciden con una información sobre amenazas encontrada en la base de datos de información de amenazas 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 "*Administración de los archivos en cuarentena*" (p. 95).

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

  Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los investigadores de amenazas de Bitdefender. Si se confirma la presencia de amenazas, se publica una actualización de información de amenazas para permitirle eliminarla.

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

Mover a Cuarentena
Traslada los archivos detectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Para más información, diríjase a "*Administración de los archivos en cuarentena*" (p. 95).

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

13.1.3. 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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. En la ventana **Escudo**, haga clic en el menú de acordeón **Mostrar ajustes avanzados**.

   Se muestra una ventana con paneles.
4. Desplácese hacia abajo por la ventana hasta que aparezca la opción **Reiniciar ajustes**. Seleccione esta opción para reiniciar los ajustes del antivirus y que adopten los valores por defecto.

13.2. Análisis solicitado

El objetivo principal de Bitdefender es mantener su equipo limpio de amenazas. Esto se consigue manteniendo las nuevas amenazas fuera de su equipo 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 equipo en busca de amenazas preexistentes nada más instalar Bitdefender. Y, desde luego, es buena idea analizar frecuentemente su equipo 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 equipo siempre que quiera ejecutando las tareas predeterminadas o sus propias tareas de análisis (tareas definidas por el usuario). Si desea analizar ubicaciones específicas en el equipo o configurar las opciones de análisis, configure y ejecute un análisis personalizado.

13.2.1. Analizar un archivo o una carpeta en busca de amenazas

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

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

13.2.2. 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 panel **ANTIVIRUS**, haga clic en **QuickScan**.
3. 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.

13.2.3. Ejecución de un análisis del sistema

La tarea de análisis del sistema analiza todo el equipo 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 equipo.

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 equipo 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 "*Mantenimiento de Bitdefender al día*" (p. 41).
- Cierre todos los programas abiertos.

Si desea analizar ubicaciones específicas en su equipo o configurar las opciones de análisis, configure y ejecute un análisis personalizado. Para

más información, diríjase a "*Configuración de un análisis personalizado*" (p. 83).

Para ejecutar un Análisis del sistema:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Análisis del sistema**.
3. La primera vez que ejecuta un Análisis del sistema, se le presenta esta característica. Haga clic en **BIEN, ENTENDIDO** para continuar.
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.

13.2.4. Configuración de un análisis personalizado

En la ventana **Administrar análisis**, puede configurar Bitdefender para que ejecute análisis siempre que considere que su equipo 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.

Cuando acceda a la ventana, tendrá a su disposición los siguientes iconos:

La tarea de análisis programado está desactivada.

La tarea de análisis programado está activada.

Desde aquí puede llevarse a cabo la configuración detallada.

Elimine el análisis seleccionado. Esta opción solo está disponible para nuevos análisis personalizados.

Para configurar detalladamente un nuevo análisis personalizado:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Administrar análisis**.
3. Haga clic en **Crear una nueva tarea de 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:
   - **Analizar únicamente aplicaciones**. Puede configurar Bitdefender para analizar solo las apps 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 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. Habilite **Programar tarea de análisis** y, a continuación, elija 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 análisis

Puede que esta información le sea útil:

- Si no se familiariza con algunos términos, compruebe estos en el glosario. También puede encontrar información de utilidad buscando en internet.
- **Analizar en busca de aplicaciones potencialmente no deseadas.** Seleccione esta opción para analizar en busca de 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 archivos comprimidos.** Los archivos que contienen archivos infectados no son amenazas inmediatas para la seguridad de sus 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. Sin embargo, recomendamos utilizar esta opción con el fin de detectar y eliminar cualquier amenaza potencial, incluso si esta no es 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.

- **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 los sectores de arranque.** Puede configurar Bitdefender para que analice los sectores de arranque de su disco duro. Este sector del disco duro contiene el código del equipo necesario para iniciar el proceso de arranque. Cuando una amenaza infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar sus sistema y acceder a sus datos.
- **Analizar memoria.** Seleccione esta opción para analizar programas que se ejecuten en la memoria de su sistema.
- **Analizar registro.** Seleccione esta opción para analizar las claves de registro. El Registro de Windows es una base de datos que almacena los ajustes de configuración y opciones para los componentes del sistema operativo Windows, además de para las aplicaciones instaladas.
- **Analizar cookies.** Seleccione esta opción para analizar las cookies almacenadas por los navegadores en su equipo.
- **Analizar keyloggers.** Seleccione esta opción para analizar su sistema en busca de aplicaciones keylogger. Los Keyloggers registran lo que escribe en el teclado y envían informes por internet a alguien con malas intenciones (hacker). El hacker puede encontrar información personal entre los datos robados, como números de cuentas bancarias o contraseñas, pudiendo utilizarlos para su propio beneficio.

13.2.5. Asistente del análisis Antivirus

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

Nota

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

Paso 1 - Ejecutar análisis

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

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

Detener o pausar el análisis. Puede detener el análisis en cualquier momento que desee haciendo clic en **DETENER**. Irá directamente al último paso del asistente. Para detener temporalmente el proceso de análisis, haga clic en **PAUSA**. Tendrá que hacer clic en **REANUDAR** para retomar el análisis.

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

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

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:

Adoptar medidas

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

- **Archivos infectados.** Los archivos detectados como infectados coinciden con una información sobre amenazas encontrada en la base de datos de información de amenazas 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 "*Administración de los archivos en cuarentena*" (p. 95).

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

Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los investigadores de amenazas de Bitdefender. Si se confirma la presencia de una amenaza, se publica una actualización de información para permitirle eliminarla.

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

Eliminar

Elimina los archivos detectados del disco.

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

Ninguna acción

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

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

Paso 3 – Resumen

Una vez Bitdefender ha finalizado la reparación de los problemas, aparecerán los resultados del análisis en una nueva ventana. Si desea información 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*" (p. 165).

13.2.6. 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. Haga clic en **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**.

13.3. Análisis automático de los medios extraíbles

Bitdefender detecta automáticamente si conecta un dispositivo de almacenamiento extraíble a su equipo, y lo analiza en segundo plano cuando está activada la opción de Autoanálisis. Esto se recomienda con el fin de evitar que su equipo 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.

13.3.1. ¿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.

Aparece un icono de análisis de Bitdefender en el área de notificación. Puede hacer clic en este icono para abrir la ventana de análisis y ver el progreso del análisis.

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 tomar 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*" (p. 165).

13.3.2. Administrar el análisis de medios extraíbles

Para gestionar el análisis automático de medios extraíbles:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Discos y dispositivos**.

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.

13.4. Analizar archivo del host

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

Para configurar el análisis del archivo hosts:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Avanzado**.
3. Active o desactive el **análisis del archivo hosts**.

13.5. 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**.

13.5.1. Exceptuar del análisis los archivos o carpetas

Para exceptuar determinados archivos y carpetas del análisis:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Excepciones**.
4. Haga clic en el menú de acordeón **Lista de archivos y carpetas exceptuados del análisis**. En la ventana que aparece puede administrar los archivos y carpetas exceptuados del análisis.
5. Añada excepciones siguiendo estos pasos:
   a. Haga clic en **Añadir**.
   b. Haga clic en **EXAMINAR**, seleccione el archivo o carpeta que desea exceptuar del análisis y, a continuación, haga clic en **AÑADIR**. Como alternativa, puede escribir (o copiar y pegar) en el campo de edición la ruta del archivo o carpeta.
   c. Por defecto, el archivo o carpeta seleccionado se exceptúa tanto en el análisis en tiempo real como en el análisis bajo demanda. Para cambiar

el momento de aplicación de la excepción, seleccione una de las otras opciones.

d. Haga clic en **Añadir**.

13.5.2. 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 equipo. 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 equipo sea vulnerable a las amenazas.

Para exceptuar extensiones de archivo del análisis:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Excepciones**.
4. Haga clic en el menú de acordeón **Lista de extensiones exceptuadas del análisis**. En la ventana que aparece puede administrar las extensiones de archivo exceptuadas del análisis.
5. Añada excepciones siguiendo estos pasos:
   a. Haga clic en **Añadir**.
   b. Escriba las extensiones que desea exceptuar del análisis, separándolas con punto y coma (;). Aquí tiene un ejemplo:

      txt;avi;jpg

   c. Por defecto, todos los archivos con las extensiones mencionadas son exceptuados tanto en el análisis en tiempo real como en el análisis bajo demanda. Para cambiar el momento de aplicación de la excepción, seleccione una de las otras opciones.
   d. Haga clic en **AÑADIR**.

13.5.3. 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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Excepciones**.
4. Utilice las opciones del menú de acordeón **Lista de archivos y carpetas exceptuados del análisis** para administrar las excepciones del análisis.
5. Para eliminar o editar excepciones del análisis, haga clic en uno de los enlaces disponibles. Siga estos pasos:
   - Para eliminar una entrada de la lista, selecciónela y haga clic en **Eliminar**.
   - Para editar un elemento de la tabla, haga doble clic en él (o selecciónelo y haga clic en **Editar**). Aparece una nueva ventana donde podrá cambiar la extensión o la ruta que desee exceptuar, así como el tipo de análisis del que desea exceptuarla. Realice los cambios necesarios y haga clic en **MODIFICAR**.

13.6. 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.

Por defecto, los archivos en cuarentena se envían automáticamente a los laboratorios de Bitdefender con el fin de ser analizados por los investigadores de amenazas de Bitdefender. Si se confirma la presencia de una amenaza, se publica una actualización de información para permitirle eliminarla.

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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Cuarentena**.

   Aquí puede ver el nombre de los archivos en cuarentena, su ubicación original y el nombre de las amenazas detectadas.
3. 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.
4. 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**.

14. ADVANCED THREAT DEFENSE

Defensa Contra Amenazas Avanzadas 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 equipo, 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.

14.1. Activar o desactivar Defensa Contra Amenazas Avanzadas

Para activar o desactivar Defensa Contra Amenazas Avanzadas:

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

> **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.

14.2. Comprobación de los ataques maliciosos detectados

Siempre que se detecten amenazas o procesos potencialmente maliciosos, Bitdefender los bloqueará para evitar que su equipo 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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.

2. En el panel **DEFENSA CONTRA AMENAZAS AVANZADAS**, haga clic en **Defensa contra amenazas**.
3. La primera vez que accede a la Protección contra ransomware, se le presenta esta característica. Haga clic en **BIEN, ENTENDIDO** para continuar.

   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.

14.3. 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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ADVANCED THREAT DEFENSE**, haga clic en **Ajustes**.
3. En el área **Excepciones**, haga clic en **Añadir aplicaciones a la lista blanca**.
4. Busque y seleccione la app que desea exceptuar y, a continuación, haga clic en **ACEPTAR**.

   Para eliminar un elemento de la lista, haga clic en la opción **Eliminar** junto a él.

14.4. 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 equipo 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:

- Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
- En el panel **ADVANCED THREAT DEFENSE**, haga clic en **Ajustes**.
- Haga clic en el conmutador correspondiente para activar o desactivar.

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

15. PREVENCIÓN DE AMENAZAS ONLINE

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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **PREVENCIÓN DE AMENAZAS ONLINE**, haga clic en **Ajustes**.

En la ventana **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 albergar contenido peligroso. Tenga cuidado si desea visitarla.

  Esta página es segura.

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

El Asesor de búsqueda califica los enlaces publicados en los siguientes servicios de redes sociales:
- Facebook
- Twitter

- Análisis de 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 el fraude.

- Protección contra phishing.

En la ventana **Prevención de amenazas de red**, tiene la opción de **Prevención de amenazas de red**. Para mantener su equipo 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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **PREVENCIÓN DE AMENAZAS ONLINE**, haga clic en **Excepciones**.
3. Escriba en el campo correspondiente el nombre del sitio web, el nombre del dominio o la dirección IP que desea añadir a las excepciones y luego haga clic en **AÑADIR**.

   Para eliminar una entrada de la lista, selecciónela y haga clic en **Eliminar**.

   Haga clic en **GUARDAR** para aplicar los cambios y cierre la ventana.

15.1. Alertas de Bitdefender en el navegador

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

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

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

- Abandone 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.

16. VULNERABILIDAD

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

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

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

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

- Puede analizar su sistema en busca de vulnerabilidades y repararlas paso a paso utilizando la opción **Análisis de vulnerabilidades**.
- Mediante la monitorización de vulnerabilidades, puede averiguar y corregir las vulnerabilidades detectadas en la ventana Notificaciones.

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

16.1. 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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VULNERABILIDADES**, haga clic en **Análisis de vulnerabilidades**.
3. La primera vez que accede al Análisis de vulnerabilidades, se le presenta esta característica. Haga clic en **INICIAR ANÁLISIS** para continuar y luego

espere a que Bitdefender compruebe su sistema para detectar vulnerabilidades.

- **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.

- **Actualizaciones 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.

- **Cuentas de Windows vulnerables**

  Puede ver la lista de las cuentas de usuario de Windows configuraras en su equipo 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 @).

- **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.

16.2. Usar el control automático de la vulnerabilidad

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

Para revisar y reparar las incidencias detectadas:

1. Haga clic en **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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VULNERABILIDADES**, haga clic en **Ajustes**.

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

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

Actualización 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.

16.3. Asesor de seguridad Wi-Fi

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

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

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

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

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

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

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

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

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VULNERABILIDADES**, haga clic en **Ajustes**.
3. En la ventana **Ajustes**, active o desactive la opción **Asesor de seguridad Wi-Fi**.

16.3.2. Configurar una red Wi-Fi doméstica

Para empezar a configurar su red doméstica:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VULNERABILIDADES**, haga clic en **Seguridad Wi-Fi**.
3. 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.
4. 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**.

16.3.3. Configurar una red Wi-Fi empresarial

Para empezar a configurar su red empresarial:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VULNERABILIDADES**, haga clic en **Seguridad Wi-Fi**.

3. 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 haya conectado hasta ese momento.

4. 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**.

16.3.4. 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 Antivirus Plus 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.

16.3.5. Revisar la información relativa a las redes Wi-Fi

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

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VULNERABILIDADES**, haga clic en **Seguridad Wi-Fi**.

3. En función de la información que necesite, seleccione una de las tres pestañas: **Wi-Fi doméstica**, **Wi-Fi empresarial** o **Wi-Fi pública**.
4. 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.

17. ARCHIVOS SEGUROS

El ransomware es un software malicioso que ataca a los sistemas vulnerables y los bloquea, con el fin de solicitar dinero al usuario a cambio de permitirle recuperar el control de su sistema. Este software malicioso actúa astutamente, mostrando mensajes falsos para que el usuario entre en pánico, instándole a efectuar el pago solicitado.

Dicha infección puede propagarse mediante spam, al descargar archivos adjuntos, o por visitar sitios web infectados e instalar apps maliciosas sin que el usuario se percate de lo que está sucediendo en su sistema.

El ransomware puede presentar cualquiera de los siguientes comportamientos que impiden que el usuario acceda a su sistema:

- Cifrar archivos confidenciales y personales sin dar la posibilidad de descifrarlos hasta que la víctima pague un rescate.
- Bloquear la pantalla del equipo y mostrar un mensaje pidiendo dinero. En este caso, no se cifra ningún archivo y simplemente se fuerza al usuario a que efectúe el pago.
- Bloquear la ejecución de apps.

Con Archivos seguros de Bitdefender puede proteger sus archivos personales contra los ataques de ransomware, como por ejemplo sus documentos, fotos o películas.

Nota

Defensa Contra Amenazas Avanzadas y Archivos seguros son dos capas de protección contra ransomware. Defensa Contra Amenazas Avanzadas es la característica que bloquea los ataques de ransomware que tratan de acceder a las áreas críticas de su sistema, mientras que Archivos seguros se cerciora de que no se cifre ningún archivo importante de su equipo.

17.1. Activar o desactivar Archivos seguros

Para activar o desactivar la característica Archivos seguros:

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

Cada vez que una aplicación intente acceder a uno de los archivos protegidos, aparecerá una ventana emergente de Bitdefender. Puede permitir o bloquear el acceso.

Nota
La característica Archivos seguros no está activada por defecto.

17.2. Proteger los archivos personales de los ataques de ransomware

Si desea poner a buen recaudo sus archivos personales:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ARCHIVOS SEGUROS**, haga clic en **Carpetas protegidas**.
3. La primera vez que accede a Carpetas protegidas, se le presenta esta característica. Haga clic en **PROTEGER MÁS CARPETAS** para continuar.
4. Seleccione la carpeta que desea proteger y, a continuación, haga clic en **Aceptar**.

   Para añadir más carpetas, haga clic en el enlace **Proteger más carpetas**. Como alternativa, arrastre las carpetas a esta ventana.

Las carpetas Imágenes, Vídeos, Música y Escritorio están protegidas por defecto contra los ataques. Los datos personales almacenados en servicios de alojamiento de archivos online, como Box, Dropbox, Google Drive y OneDrive también están incluidos en el entorno de protección, siempre que sus aplicaciones estén instaladas en el sistema.

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.

Nota
Se pueden proteger carpetas personalizadas solo para los usuarios actuales. Los archivos del sistema y de aplicaciones no se pueden añadir a las excepciones.

17.3. Configuración del acceso de las apps

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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ARCHIVOS SEGUROS**, haga clic en **Acceso de las aplicaciones**.
3. Aparecen las apps que hayan solicitado cambiar archivos de sus carpetas protegidas. Active el conmutador junto a la app que considera segura.

En la misma ventana, puede desactivar la protección contra ransomware para determinadas apps desactivando el conmutador correspondiente.

Si desea añadir nuevas aplicaciones a la lista, haga clic en el enlace **Añadir una nueva aplicación a la lista**.

17.4. Protección en el arranque

Se sabe que muchas apps maliciosas se ponen en funcionamiento al arrancar el sistema, lo que puede dañar seriamente una máquina. La Protección en el arranque de Bitdefender analiza todas las áreas críticas del sistema antes de que se carguen todos los archivos, con un impacto nulo en el sistema.

Para desactivar la protección en el arranque:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ARCHIVOS SEGUROS**, haga clic en **Ajustes**.
3. Desactive la **Protección en el arranque**.

> **Nota**
> Las apps añadidas a las excepciones también se analizarán y se tratarán en consecuencia.

18. 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.

18.1. Activación y desactivación de la Reparación de ransomware

Para activar y desactivar la Reparación de ransomware:

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.

18.2. 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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **REPARACIÓN DE RANSOMWARE**, haga clic en **Ajustes**.
3. Activar o desactivar el conmutador **Restauración automática**.

18.3. 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 equipo sin preocupaciones, sabiendo que sus archivos están a salvo.

Para ver archivos que se restauraron automáticamente:

1. Haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación referente al 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.

18.4. 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. Haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación referente al 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;

18.5. 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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **REPARACIÓN DE RANSOMWARE**, haga clic en **Ajustes**.
3. Para añadir nuevas aplicaciones a la lista, haga clic en **Añadir una nueva aplicación a la lista**.

19. PROTECCIÓN DEL GESTOR DE CONTRASEÑAS PARA SUS CREDENCIALES

Usamos nuestros equipos para comprar online o pagar nuestras facturas, para conectarnos a plataformas de redes sociales o iniciar sesión con aplicaciones de mensajería instantánea.

¡Pero como todo el mundo sabe, no siempre es fácil recordar una contraseña!

Y si no tenemos cuidado mientras navegamos online, nuestra información privada, como nuestra dirección de correo, nuestro ID de mensajería instantánea o los datos de nuestra tarjeta de crédito pueden verse comprometidos.

Guardar sus contraseñas o sus datos personales en una hoja de papel o en el equipo puede ser peligroso porque pueden acceder a ellos personas que quieran robar y usar esa información. Y recordar todas las claves que haya establecido para sus cuentas online o para sus sitios Web favoritos no es una tarea fácil.

Por consiguiente, ¿hay alguna manera de asegurar que podamos encontrar nuestras contraseñas siempre que las necesitemos? ¿Y podamos descansar tranquilos sabiendo que nuestras contraseñas secretas están siempre a salvo?

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

Utilizando una única contraseña maestra para acceder a sus credenciales, el Gestor de contraseñas le facilita mantener sus contraseñas a salvo en un Wallet.

Para ofrecer la mejor protección para sus actividades online, el Gestor de contraseñas se integra con Bitdefender Safepay™ y proporciona una solución única para las distintas formas en las que puede comprometerse su información privada.

El Gestor de contraseñas protege la siguiente información privada:

- Información personal, tal como la dirección de e-mail o el número de teléfono
- Credenciales de inicio de sesión en sitios Web
- Información de cuentas bancarias o números de tarjetas de crédito

- Datos de acceso a cuentas de correo
- Contraseñas para apps
- Contraseñas para las redes Wi-Fi

19.1. Crear una nueva base de datos de Wallet

El Wallet de Bitdefender es el lugar donde puede guardar sus datos personales. Para facilitar su experiencia de navegación, debe crear una base de datos de Wallet de la siguiente manera:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Crear nuevo wallet**.
3. Haga clic en **Crear nuevo**.
4. Introduzca la información requerida en los campos correspondientes.
   - Etiqueta de Wallet: escriba un nombre único para su base de datos de Wallet.
   - Contraseña maestra: introduzca una contraseña para su Wallet.
   - Repetir contraseña: vuelva a escribir la contraseña que estableció.
   - Pista: escriba una pista para recordar la contraseña.
5. Haga clic en **CONTINUAR**.
6. En este paso puede optar por almacenar su información en la nube. Si selecciona Sí, la información bancaria permanecerá almacenada localmente en su dispositivo. Elija la opción deseada y, a continuación, haga clic en **CONTINUAR**.
7. Seleccione el navegador Web desde el que desea importar las credenciales.
8. Haga clic en **FINALIZAR**.

19.2. Importar una base de datos existente

Para importar una base de datos de Wallet almacenada localmente:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Crear nuevo wallet**.

3. Haga clic en **DESDE OBJETIVO**.
4. Diríjase a la ubicación de su dispositivo donde desee guardar la base de datos de Wallet y, a continuación, elija un nombre para ella.
5. Haga clic en **Abrir**.
6. Otorgue un nombre a su Wallet y escriba la contraseña que se le asignó durante su creación inicial.
7. Haga clic en **IMPORTAR**.
8. Seleccione los programas desde los que desea que Wallet importe las credenciales y, a continuación, pulse el botón **FINALIZAR**.

19.3. Exportar la base de datos de Wallet

Para exportar la base de datos de su Wallet:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Mis wallets**.
3. Haga clic en el icono ⋮ del Wallet deseado y, a continuación, seleccione **Exportar**.
4. Busque la ubicación de su base de datos de Wallet y selecciónela (el archivo .db).
5. Haga clic en **Guardar**.

Nota
Para que la opción **Exportar** esté disponible, ha de estar abierto el Wallet. Si el Wallet que necesita exportar está bloqueado, haga clic en **ACTIVAR WALLET** y, a continuación, escriba la contraseña que se le asignó durante su creación inicial.

19.4. Sincronización de sus Wallets en la nube

Para activar o desactivar la sincronización de Wallets en la nube:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Mis wallets**.

3. Haga clic en el icono ⋮ del Wallet deseado y, a continuación, seleccione **Ajustes**.
4. Elija la opción que desee en la ventana que aparece y, a continuación, haga clic en **Guardar**.

> **Nota**
> Para que la opción **Exportar** esté disponible, ha de estar abierto el Wallet. Si el Wallet que necesita sincronizar está bloqueado, haga clic en **ACTIVAR WALLET** y, a continuación, escriba la contraseña que se le asignó durante su creación inicial.

19.5. Administrar sus credenciales de Wallet

Para administrar sus contraseñas:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Mis wallets**.
3. Seleccione la base de datos de Wallet deseada y, a continuación, haga clic en **ACTIVAR WALLET**.
4. Escriba la contraseña maestra y, a continuación, haga clic en **Aceptar**.

Aparecerá una nueva ventana. Seleccione la categoría deseada desde la parte superior de la ventana:

- Identidad
- Sitios Web
- Banca online
- Direcciones
- Apps
- Redes Wi-Fi

Añadir/Modificar las credenciales

- Para añadir una contraseña nueva, escoja arriba la categoría deseada, haga clic en **+ Añadir elemento**, inserte la información en los campos correspondientes y haga clic en el botón Guardar.

- Para editar un elemento de la tabla, selecciónelo y haga clic en el botón **Editar**.
- Para eliminar una entrada, selecciónela y haga clic en el botón **Eliminar**.

19.6. Activar o desactivar la protección del Gestor de contraseñas

Para activar o desactivar la protección del Gestor de contraseñas:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, active o desactive el conmutador.

19.7. Administración de los ajustes del Gestor de contraseñas

Para configurar en detalle la contraseña maestra:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Ajustes de seguridad**.

Tiene las siguientes opciones a su disposición:

- **Pedir mi contraseña maestra cuando inicie sesión en mi dispositivo** - se le pedirá que escriba su contraseña maestra cuando acceda al dispositivo.
- **Pedir mi contraseña maestra cuando abra mi navegador y apps** - se le pedirá que escriba su contraseña maestra cuando acceda a un navegador o a una aplicación.
- **No pedir mi contraseña maestra**: No se le pedirá que escriba su contraseña maestra cuando acceda al equipo, a un navegador o a una app.
- **Bloquear automáticamente Wallet cuando deje mi dispositivo desatendido** - se le pedirá que escriba su contraseña maestra cuando vuelva a su dispositivo tras 15 minutos.

Importante
Asegúrese de recordar su contraseña maestra o guardar registro de ella en un lugar seguro. Si olvidó la contraseña, deberá reinstalar el programa o ponerse en contacto con Bitdefender para recibir ayuda.

Mejore su experiencia

Para seleccionar los navegadores o las aplicaciones donde quiera integrar el Gestor de contraseñas:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Plugins**.

   Marque una aplicación para usar el Gestor de contraseñas y mejorar su experiencia:

   - Internet Explorer
   - Mozilla Firefox
   - Google Chrome
   - Safepay

Configurar Autocompletar

La característica Autocompletar facilita conectar con sus sitios Web favoritos o iniciar sesión en sus cuentas online. La primera vez que introduzca sus credenciales de acceso e información personal en su navegador Web, se protegerán automáticamente en Wallet.

Para configurar las opciones de **Autocompletar**:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **GESTOR DE CONTRASEÑAS**, haga clic en **Ajustes**.
3. Seleccione la pestaña **Configuración de autocompletar**.
4. Configure de las opciones siguientes:

   - **Configurar la forma en que el Gestor de contraseñas protege sus credenciales**:

- **Guardar las credenciales automáticamente en Wallet** - las credenciales de inicio de sesión y otra información de identificación, como sus datos personales y de tarjetas de crédito, se guardan y actualizan automáticamente en Wallet.
- **Preguntarme siempre** - se le preguntará cada vez que quiera añadir sus credenciales a Wallet.
- **No guardar, actualizaré la información manualmente** - las credenciales pueden añadirse únicamente de forma manual en Wallet.

- **Autocompletar credenciales de inicio de sesión**:
  - **Autocompletar credenciales de inicio de sesión siempre** - las credenciales se introducen automáticamente en el navegador.
- **Autocompletar formularios**:
  - **Preguntar mis opciones de completado cuando visito una página con formularios** - aparecerá una ventana emergente con las opciones de completado cada vez que Bitdefender detecte que desea realizar un pago online o un registro.

Administrar la información del Gestor de contraseñas desde su navegador

Puede administrar fácilmente la información del Gestor de contraseñas directamente desde su navegador, para que tenga a mano todos sus datos importantes. El complemento Wallet de Bitdefender es compatible con los siguientes navegadores: Google Chrome, Internet Explorer y Mozilla Firefox, y también va integrado en Safepay.

Para acceder a la extensión Wallet de Bitdefender, abra su navegador Web, permita que se instale el complemento y haga clic en el icono de la barra de herramientas.

La extensión Wallet de Bitdefender contiene las siguientes opciones:

- Abrir Wallet - abre Wallet.
- Bloquear Wallet - bloquea Wallet.
- Páginas Web - abre un submenú con todos los inicios de sesión en sitios Web almacenados en Wallet. Haga clic en **Añadir página Web** para añadir nuevos sitios Web a la lista.

- Rellenar formularios - abre un submenú que contiene la información añadida por usted para una categoría determinada. Desde aquí puede añadir nuevos datos a su Wallet.
- Generador de contraseñas: le permite generar contraseñas aleatorias que puede utilizar para cuentas nuevas o existentes. Haga clic en **Mostrar ajustes avanzados** para personalizar la complejidad de la contraseña.
- Ajustes: abre la ventana de ajustes del Gestor de contraseñas.
- Informar de un problema: informe de cualquier problema que encuentre con el Gestor de contraseñas de Bitdefender.

20. 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:

- Internet Explorer
- 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.

20.1. 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.

20.2. 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 de la esquina superior derecha.
  4. Utilice el conmutador correspondiente para desactivarlo.

     El icono de Bitdefender se vuelve gris.
- Desde la interfaz de Bitdefender:
  1. Haga clic en **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.

20.3. 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. Abra su navegador Web.
2. Haga clic en el icono junto a la barra de búsqueda.
3. Haga clic en el icono de 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 .

21. VPN

Puede instalar la aplicación VPN desde su producto Bitdefender y usarla cada vez que desee añadir una capa más de protección a su conexión. 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 Bitdefender 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.

21.1. Instalación de VPN

Puede instalar la app VPN desde la interfaz de Bitdefender de la siguiente manera:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **VPN**, haga clic en **Instalar VPN**.
3. En la ventana con la descripción de la app VPN, lea el **Acuerdo de suscripción** y, a continuación, haga clic en **INSTALAR BITDEFENDER VPN**.

   Espere unos momentos a que se descarguen e instalen los archivos.

   Si se detecta otra aplicación VPN, le recomendamos que la desinstale. Si tiene instaladas varias soluciones VPN, es posible que se produzcan demoras en el sistema u otros problemas de funcionamiento.
4. Haga clic en **ABRIR BITDEFENDER VPN** para finalizar el proceso de instalación.

Nota
Bitdefender VPN requiere la instalación de .Net Framework 4.5.2 o superior. En caso de que no tenga instalado este paquete, aparecerá una ventana de notificación. Haga clic en **instalar .Net Framework** para que se le redirija a una página desde donde puede descargar la versión más reciente de este software.

21.2. Abrir VPN

Para acceder a la interfaz principal de Bitdefender VPN, utilice uno de los siguientes métodos:

- Desde el área de notificación
  1. Haga clic con el botón derecho en el icono del área de notificación y, a continuación, haga clic en **Mostrar**.
- Desde la interfaz de Bitdefender:
  1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
  2. En el panel **VPN**, haga clic en **Abrir VPN**.

21.3. Interfaz de VPN

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 premium tienen la posibilidad de cambiar la ubicación del servidor al que deseen conectarse. Para obtener más información sobre las suscripciones a VPN, consulte "*Suscripciones*" (p. 131).

Para conectarse o desconectarse, basta con hacer clic en el estado que se muestra en la parte superior de la pantalla o hacer clic con el botón derecho en el icono del área de notificación. El icono del área de notificación muestra una marca de verificación verde cuando la VPN está conectada y una roja cuando no lo está.

Mientras está conectado, el tiempo transcurrido y el uso de ancho de banda se muestran en la parte inferior de la interfaz.

Para disponer de más opciones, acceda al **Menú** haciendo clic en el icono de la zona superior derecha. Aquí tiene las siguientes opciones:

- **Mi cuenta**: se muestran los detalles sobre su cuenta de Bitdefender y su suscripción a VPN. Haga clic en **Cambiar cuenta** si desea iniciar sesión con otra distinta.
- **Ajustes**: puede personalizar el comportamiento de su producto según sus necesidades:
  - Recibir notificaciones cuando la VPN se conecta o desconecta automáticamente.
  - ejecutar automáticamente la app VPN al inicio de Windows
  - iniciar automáticamente la app VPN cuando su dispositivo se conecte a redes inalámbricas inseguras
- **Actualizar a Premium**: si utiliza la versión gratuita, puede actualizar al plan premium desde aquí.
- **Soporte**: se le redirige a la plataforma de nuestro Centro de soporte, donde puede leer un artículo sobre cómo usar Bitdefender VPN.
- **Acerca de** : Muestra información acerca de la versión instalada.

21.4. 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 más adecuado.

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 **CONSEGUIR TRÁFICO ILIMITADO** disponible en la interfaz del producto.

La suscripción a Bitdefender Premium VPN es independiente de la suscripción a Bitdefender Antivirus Plus, lo que significa que podrá usarla en toda su extensión independientemente del estado de la suscripción de la solución de seguridad. En caso de que caduque la suscripción a Bitdefender Premium VPN, pero la de Bitdefender Antivirus Plus siga activa, se le revertirá al plan gratuito.

Bitdefender VPN es un producto multiplataforma, disponible en 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.

22. SEGURIDAD SAFEPAY PARA LAS TRANSACCIONES ONLINE

El PC se está convirtiendo rápidamente en la herramienta para compras y banca electrónica. Pagar facturas, transferir dinero, comprar prácticamente todo lo que pueda imaginar nunca ha sido más fácil y rápido.

Esto supone enviar información personal, de cuenta y datos de la tarjeta de crédito, contraseñas y otro tipo de información privada a través de Internet, en otras palabras, exactamente el tipo de información en la que los cibercriminales están interesados. Los hackers son implacables en sus esfuerzos para robar esta información, por lo que nunca se es demasiado cuidadoso a la hora de proteger las transacciones en línea.

Bitdefender Safepay™ es sobre todo un navegador protegido, un entorno sellado que está diseñado para mantener privadas y seguras sus operaciones de banca online, compras online y cualquier otro tipo de transacción online.

Para la mejor protección de la privacidad, se ha integrado el Gestor de contraseñas de Bitdefender en Bitdefender Safepay™, con el fin de proteger sus credenciales siempre que desee acceder a ubicaciones privadas online. Para más información, diríjase a *"Protección del Gestor de contraseñas para sus credenciales"* (p. 118).

Bitdefender Safepay™ ofrece las siguientes opciones:

- Bloquea el acceso a su escritorio y cualquier intento de tomar capturas de su pantalla.
- Protege sus contraseñas secretas mientras navega por Internet con el Gestor de contraseñas.
- Viene con un teclado virtual que, cuando se utiliza, hace imposible a los hackers leer sus pulsaciones en el teclado.
- Es completamente independiente de sus otros navegadores.
- Viene con una función de protección de punto de acceso para cuando su equipo esté conectado a redes Wi-Fi no seguras.
- Acepta marcadores y le permite navegar entre sus sitios favoritos de banca y compras.
- No está limitado a banca electrónica y compras por Internet. Puede abrirse cualquier sitio Web en Bitdefender Safepay™.

22.1. Utilizar Bitdefender Safepay™

Por omisión, Bitdefender detecta cuando navega hacia una página de un banco online o a una tienda online en cualquier navegador de su equipo y le pide que la lance en Bitdefender Safepay™.

Para acceder a la interfaz principal de Bitdefender Safepay™, utilice uno de los siguientes métodos:

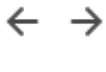
- Desde la interfaz de Bitdefender:
  1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
  2. En el panel **SAFEPAY**, haga clic en **Abrir Safepay**.
- En Windows:
  - En **Windows 7**:
    1. Haga clic en **Inicio** y diríjase a **Todos los programas**.
    2. Haga clic en **Bitdefender**.
    3. Haga clic en **Bitdefender Safepay™**.
  - En **Windows 8 y Windows 8.1**:

    Localice Bitdefender Safepay™ desde la pantalla de inicio de Windows (por ejemplo puede empezar escribiendo "Bitdefender Safepay" en la pantalla Inicio) y luego haga clic en el icono.
  - En **Windows 10**:

    Escriba "Bitdefender Safepay™" en el cuadro de búsqueda de la barra de tareas y haga clic en su icono.

Si está acostumbrado a los navegadores Web, no tendrá ningún problema utilizando Bitdefender Safepay™ - se parece y se comporta igual que cualquier navegador:

- introduzca las URLs a las que desea ir en la barra de direcciones.
- añada pestañas para visitar múltiples sitios Web en la ventana de Bitdefender Safepay™ haciendo clic en  .

- navegue atrás y hacia delante y refresque las páginas usando  respectivamente.
- acceda a los ajustes de Bitdefender Safepay™ haciendo clic en y seleccionando **Ajustes**.
- Proteja sus contraseña con el Gestor de contraseñas haciendo clic en  .
- administre sus marcadores haciendo clic  junto a la barra de dirección.
- abra el teclado virtual haciendo clic en  .
- aumente o disminuya el tamaño del navegador pulsando simultáneamente **Ctrl** y las teclas **+/-** del teclado numérico.
- vea información sobre su producto Bitdefender haciendo clic en y eligiendo **Acerca de**.
- imprima la información importante haciendo clic en y eligiendo **Imprimir**.

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

22.2. 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 CERTIFICADOS** 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.

22.3. Administración de marcadores

Si ha deshabilitado la detección automática para algunos o todos los sitios Web, o Bitdefender simplemente no detecta ciertas sitios Web, puede añadir marcadores a Bitdefender Safepay™ para poder abrir con facilidad sus sitios Web favoritos en el futuro.

Siga estos pasos para añadir una URL a los marcadores de Bitdefender Safepay™:

1. Haga clic en el icono  junto a la barra de direcciones para abrir la página de marcadores.

   Nota
   La página de marcadores aparece abierta por omisión cuando inicia Bitdefender Safepay™.

2. Haga clic en el botón **+** para añadir un nuevo marcador.
3. 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.

22.4. 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. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **SAFEPAY**, haga clic en **Ajustes**.
3. Desactivar las **notificaciones de Safepay**.

22.5. Uso de VPN con Safepay

Para realizar pagos online en un entorno seguro mientras está conectado a redes inseguras, el producto de Bitdefender puede configurarse para iniciar automáticamente la app VPN al mismo tiempo que Safepay.

Para usar la app VPN junto con Safepay:

1. Haga clic en **Privacidad** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **SAFEPAY**, haga clic en **Ajustes**.

3. Active **Usar VPN con Safepay**.

23. PROTECCIÓN DE DATOS

23.1. Eliminar archivos de forma permanente

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

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

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

1. Haga clic con el botón derecho en el archivo o carpeta que desee eliminar permanentemente.
2. Seleccione **Bitdefender** > **Destructor de archivos** en el menú contextual que aparece.
3. Haga clic en **ELIMINAR PERMANENTEMENTE** y, a continuación, confirme que desea continuar con el proceso.

   Espere a que Bitdefender finalice la destrucción de 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. Haga clic en **Privacidad** 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 finalice la destrucción de archivos.

c. **Resumen de resultados**

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

24. BITDEFENDER USB IMMUNIZER

La opción de Autorun integrada en el sistema operativo Windows es una herramienta muy útil que permite a los equipos ejecutar automáticamente un archivo de un medio conectado a él. Por ejemplo, las instalaciones de software pueden comenzar automáticamente cuando se inserta un CD en la unidad óptica.

Desgraciadamente, esta opción pueden también utilizarla las amenazas para ejecutarse automáticamente e infiltrarse en su equipo desde un medio reescribible como una unidad flash USB y tarjetas conectadas mediante lectores de tarjetas. En los últimos años se han producido numerosos ataques basados en la autoejecución.

Con el inmunizador USB puede evitar que ninguna unidad flash formateada con NTFS, FAT32 o FAT vuelva a ejecutar amenazas nunca más. Una vez que el dispositivo USB está inmunizado, las amenazas no pueden volver a configurarlo para ejecutar cierta aplicación cuando el dispositivo se conecte a un equipo con Windows.

Para inmunizar un dispositivo USB:

1. Conecte la unidad flash a su equipo.
2. Examine su equipo para localizar el dispositivo de almacenamiento extraíble y haga clic con el botón derecho en su icono.
3. En el menú contextual, escoja **Bitdefender** y seleccione **Inmunizar esta unidad**.

> **Nota**
> Si la unidad ya se inmunizó, aparecerá el mensaje **El dispositivo USB está protegido contra amenazas de?ejecución automática** en vez de la opción Inmunizar.

Para evitar que su equipo ejecute amenazas desde dispositivos USB no inmunizados, desactive la opción de autoarranque del dispositivo. Para más información, diríjase a "*Usar el control automático de la vulnerabilidad*" (p. 105).

OPTIMIZACIÓN DEL SISTEMA

25. PERFILES

Las actividades de trabajo diarias, ver películas o utilizar juegos pueden provocar que el sistema se ralentice, especialmente si se están ejecutando de manera simultánea con los procesos de actualización de Windows y las tareas de mantenimiento. Con Bitdefender, ahora puede elegir y aplicar su perfil preferido, lo que lleva a cabo los ajustes del sistema adecuados para aumentar el rendimiento de las aplicaciones específicas instaladas.

Bitdefender ofrece los siguientes perfiles:

- Perfil de Trabajo
- Perfil de Películas
- Perfil de Juego
- Perfil de redes Wi-Fi públicas
- Perfil del modo Batería

Si decide no utilizar los **Perfiles**, se activa un perfil por defecto denominado **Estándar** que no aporta optimización a su sistema.

Según su actividad, se aplican los siguientes ajustes del producto cuando se activa el perfil de trabajo, juego o ver películas:

- Todas las alertas y ventanas emergentes de Bitdefender quedan desactivadas.
- Se pospone la actualización automática.
- Se posponen los análisis programados.
- Se deshabilita el Asesor de búsquedas.
- Las 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 Antivirus Plus 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

25.1. Perfil de Trabajo

La ejecución de varias tareas en el trabajo, como el envío de mensajes de correo electrónico, mantener una videoconferencia con sus compañeros o trabajar con aplicaciones de diseño puede afectar al rendimiento del sistema. El Perfil de trabajo se ha diseñado para ayudarle a mejorar su eficiencia en el trabajo, desactivando algunos de sus servicios en segundo plano y tareas de mantenimiento.

Configuración del Perfil de trabajo

Para configurar las acciones a llevar a cabo en el Perfil de trabajo:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
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. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Haga clic en el botón **CONFIGURAR** del área del 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.

25.2. Perfil de Películas

Mostrar vídeo de alta calidad, como por ejemplo películas de alta definición, requiere unos recursos del sistema significativos. El Perfil de películas ajusta la configuración del sistema y del producto para que pueda disfrutar de una experiencia cinematográfica óptima y sin interrupciones.

Configuración del Perfil de películas

Para configurar las acciones a llevar a cabo en el Perfil de películas:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Haga clic en el botón **CONFIGURAR** del área del Perfil de películas.
4. Elija los ajustes del sistema que desea aplicar marcando las siguientes opciones:
   - Aumentar el rendimiento en reproductores de vídeo

- Optimizar los ajustes del producto para el perfil de Películas
- Posponer los programas en segundo plano y las tareas de mantenimiento
- Posponer actualizaciones automáticas de Windows
- Ajustar el plan de energía para películas

5. Haga clic en **GUARDAR** para aplicar los cambios y cierre 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. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Haga clic en el botón **CONFIGURAR** del área del Perfil de películas.
4. En la ventana **Ajustes del perfil de películas**, haga clic en **Lista de reproductores**.
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.

25.3. Perfil de Juego

Disfrutar de una experiencia de juego ininterrumpido supone reducir la carga del sistema y disminuir cualquier posible retraso. Recurriendo a la heurística de comportamientos y a una lista de juegos conocidos, Bitdefender puede detectar automáticamente los juegos que se ejecuten y optimizar los recursos del sistema para que pueda disfrutar de su pausa para jugar.

Configuración del Perfil de juego

Para configurar las acciones que desea llevar a cabo en el Perfil de juego:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Haga clic en el botón **CONFIGURAR** del área del Perfil de juego.
4. Elija los ajustes del sistema que desea aplicar marcando las siguientes opciones:
   - Aumentar el rendimiento en los juegos
   - Optimizar los ajustes del producto para el perfil de Juego
   - Posponer los programas en segundo plano y las tareas de mantenimiento
   - Posponer actualizaciones automáticas de Windows
   - Ajustar el plan de energía para juegos
5. Haga clic en **GUARDAR** para aplicar los cambios y cierre 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 **Lista de aplicaciones de juego**.

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

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
3. Haga clic en el botón **CONFIGURAR** del área del Perfil de juego.
4. En la ventana **Ajustes del perfil de juego**, haga clic en **Lista de juegos**.
5. Haga clic en **AÑADIR**.

   Aparecerá una nueva ventana. Busque el archivo ejecutable del juego, selecciónelo y haga clic en **Aceptar** para añadirlo a la lista.

25.4. Perfil de redes Wi-Fi públicas

Enviar correos electrónicos, escribir credenciales confidenciales o efectuar compras online mientras se está conectado a redes inalámbricas poco

fiables puede poner en riesgo sus datos personales. El perfil de redes Wi-Fi públicas adapta los ajustes del producto para darle la posibilidad de realizar pagos online y hacer uso de información confidencial en un entorno protegido.

Configuración del perfil de redes Wi-Fi públicas

Para configurar Bitdefender de forma que aplique los ajustes del producto mientras está conectado a una red inalámbrica poco fiable:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
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. Haga clic en **Guardar**.

25.5. Perfil del modo Batería

El perfil del modo Batería está especialmente diseñado para usuarios de portátiles y tablets. Su objetivo es reducir al mínimo tanto el impacto del sistema como de Bitdefender en el consumo de energía cuando el nivel de carga de la batería esté por debajo del establecido por omisión o del que usted determine.

Configuración del perfil del modo Batería

Para configurar el perfil del modo Batería:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.
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. Haga clic en **GUARDAR** para aplicar los cambios y cierre la ventana.

Escriba un valor válido en el cuadro de número o selecciónelo con las teclas de flecha arriba y abajo para especificar cuándo debe empezar a funcionar el sistema en modo Batería. Por defecto, el modo se activa cuando el nivel de carga de la batería cae por debajo del 30%.

Cuando Bitdefender opera en el perfil del modo Batería, se aplican los siguientes ajustes del producto:

- Se pospone la actualización automática de Bitdefender.
- Se posponen los análisis programados.
- Se desactiva el Widget de seguridad.

Bitdefender detecta cuándo su portátil pasa a la alimentación con batería y, en función del nivel de carga de ésta, entra automáticamente en modo Batería. De la misma forma, Bitdefender sale automáticamente del modo Batería cuando detecta que el portátil ya no está siendo alimentado con la batería.

25.6. Optimización en tiempo real

La Optimización en tiempo real de Bitdefender es un plugin que mejora el rendimiento de su sistema discretamente, en segundo plano, asegurándose de que no se vea interrumpido mientras esté en un modo de perfil. Dependiendo de la carga de la CPU, el plugin monitoriza todos los procesos, centrándose en los que suponen una carga mayor, para adaptarlos a sus necesidades.

Para activar o desactivar la Optimización en tiempo real:

1. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Perfiles**.

3. Desplácese hacia abajo hasta ver la opción de Optimización en tiempo real y, a continuación, utilice el conmutador correspondiente para activarla o desactivarla.

RESOLUCIÓN DE PROBLEMAS

26. RESOLUCIÓN DE INCIDENCIAS COMUNES

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

Si no puede encontrar su problema aquí, o si las soluciones presentadas no lo resuelven, puede contactar con los representantes de servicio técnico de Bitdefender como se presenta en el capítulo "*Pedir ayuda*" (p. 176).

26.1. Mi sistema parece que se ejecuta lento

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

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

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

  Aunque Bitdefender 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?*" (p. 71).

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

  Si su equipo 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*" (p. 3).

- **Ha instalado apps que no utiliza**.

  Cualquier equipo tiene programas o apps 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 equipo. Asegúrese de que puede analizar su sistema periódicamente, al menos una vez a la semana. Se recomienda utilizar el análisis de sistema Bitdefender porque analiza todo los tipos de amenazas que ponen en peligro la seguridad de su sistema.

  Para iniciar el análisis del sistema:

  1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
  2. En el panel **ANTIVIRUS**, haga clic en **Análisis del sistema**.
  3. Siga los pasos del asistente.

26.2. El análisis no se inicia

Este tipo de incidencia puede tener dos causas principales:

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

En este caso, reinstale Bitdefender:

- En **Windows 7**:
  1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
  2. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
  3. Haga clic en **REINSTALAR** en la ventana que aparece.
  4. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.
- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Desinstalar un programa** o **Programas y características**.
  3. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
  4. Haga clic en **REINSTALAR** en la ventana que aparece.
  5. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.
- En **Windows 10**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
  3. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
  4. Haga clic en **Desinstalar** para confirmar su elección.
  5. Haga clic en **REINSTALAR** en la ventana que aparece.
  6. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.

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.

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

  En este caso:

  1. Eliminar las otras soluciones de seguridad. Para más información, diríjase a "*¿Cómo desinstalo otras soluciones de seguridad?*" (p. 71).
  2. Reinstalar Bitdefender:
     - En **Windows 7**:
       a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
       b. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
       c. Haga clic en **REINSTALAR** en la ventana que aparece.
       d. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.
     - En **Windows 8 y Windows 8.1**:
       a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
       b. Haga clic en **Desinstalar un programa** o **Programas y características**.
       c. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
       d. Haga clic en **REINSTALAR** en la ventana que aparece.
       e. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.
     - En **Windows 10**:
       a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
       b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
       c. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
       d. Haga clic en **Desinstalar** para confirmar su elección.
       e. Haga clic en **REINSTALAR** en la ventana que aparece.
       f. Espere a que finalice el proceso de reinstalación y, luego, reinicie su sistema.

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.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 176).

26.3. 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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ADVANCED THREAT DEFENSE**, haga clic en **Ajustes**.
3. En el área **Excepciones**, haga clic en **Añadir aplicaciones a la lista blanca**.
4. Busque y seleccione la app que desea exceptuar y, a continuación, haga clic en **ACEPTAR**.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 176).

26.4. 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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **PREVENCIÓN DE AMENAZAS ONLINE**, haga clic en **Excepciones**.
3. Proporcione la dirección del sitio web, nombre de dominio, dirección IP o aplicación online bloqueados en el campo correspondiente y haga clic en **AÑADIR**.
4. Haga clic en **GUARDAR** para aplicar los cambios y cierre 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 le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 176).

26.5. Qué hacer si Bitdefender detecta una aplicación segura como si fuera ransomware

El ransomware es un programa malicioso que trata de obtener dinero de los usuarios mediante el bloqueo de sus sistemas vulnerables. Para mantener su sistema a salvo de situaciones desafortunadas, Bitdefender le da la posibilidad de proteger sus archivos personales.

Cuando una aplicación intente cambiar o eliminar alguno de sus archivos protegidos, se considerará poco fiable y Bitdefender bloqueará su funcionamiento.

En caso de que se añada alguna app a la lista de apps que no son de fiar y que esté seguro de que no hay problema en usarla, siga estos pasos:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ARCHIVOS SEGUROS**, haga clic en **Acceso de las aplicaciones**.
3. Aparecen las apps que hayan solicitado cambiar archivos de sus carpetas protegidas. Haga clic en el conmutador **Permitir** junto a la app que considera segura.

26.6. 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. Haga clic en **Ajustes** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Actualizar**.
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.

26.7. Los servicios de Bitdefender no responden

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

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

- La ventana de Bitdefender le indica que los servicios de Bitdefender no responden.

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

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

Para solucionar este problema, pruebe estas soluciones:

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

   Para más información, diríjase a "*¿Cómo desinstalo otras soluciones de seguridad?*" (p. 71).

Si el error persiste y contacte con nuestros representantes de soporte para conseguir ayuda según se describe en la sección "*Pedir ayuda*" (p. 176).

26.8. El Autorrellenado de mi Wallet no funciona

Ha guardado sus credenciales online en su Gestor de contraseñas de Bitdefender y se ha dado cuenta de que el autorrelenado no funciona. Normalmente, este problema se produce cuando la extensión Wallet Bitdefender no está instalada en su navegador.

Para resolver esta situación, siga estos pasos:

- En **Internet Explorer:**

  1. Abrir Internet Explorer.
  2. Haga clic en Herramientas.
  3. Haga clic en Barras de herramientas y extensiones.
  4. Haga clic en Barras de herramientas y extensiones.

5. Seleccione **Wallet de Bitdefender** y haga clic en **Activar**.

- En **Mozilla Firefox:**
  1. Abra Mozilla Firefox.
  2. Haga clic en Herramientas.
  3. Haga clic en Complementos.
  4. Haga clic en Extensiones.
  5. Seleccione **Wallet de Bitdefender** y haga clic en **Activar**.
- En **Google Chrome:**
  1. Abra Google Chrome.
  2. Vaya al icono Menú.
  3. Haga clic en Más herramientas.
  4. Haga clic en Extensiones.
  5. Seleccione **Wallet de Bitdefender** y haga clic en **Activar**.

Nota
El complemento se habilitará después de que reinicie su navegador.

Ahora compruebe si el autorrelenado de Wallet funciona con sus cuentas online.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 176).

26.9. La desinstalación de Bitdefender ha fallado

Si desea desinstalar su producto Bitdefender y observa que el proceso se cuelga o se bloquea el sistema, haga clic en **Cancelar** para cancelar la acción. Si esto no funciona, reinicie el sistema.

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

Para eliminar Bitdefender de su sistema por completo:

- En **Windows 7**:

1. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
2. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
3. Haga clic en **ELIMINAR** en la ventana que aparece.
4. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

- En **Windows 8 y Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Desinstalar un programa** o **Programas y características**.
  3. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
  4. Haga clic en **ELIMINAR** en la ventana que aparece.
  5. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
- En **Windows 10**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
  3. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
  4. Haga clic en **Desinstalar** para confirmar su elección.
  5. Haga clic en **ELIMINAR** en la ventana que aparece.
  6. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

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

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

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

Así es como puede abordar cada situación:

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

  Para resolver esto:

  1. Reinicie su sistema e inicie en Modo Seguro. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 72).
  2. Desinstalar Bitdefender de su sistema:
     - En **Windows 7**:
       a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
       b. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
       c. Haga clic en **ELIMINAR** en la ventana que aparece.
       d. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
       e. Reinicie su sistema en modo normal.
     - En **Windows 8 y Windows 8.1**:
       a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
       b. Haga clic en **Desinstalar un programa** o **Programas y características**.
       c. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.
       d. Haga clic en **ELIMINAR** en la ventana que aparece.
       e. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
       f. Reinicie su sistema en modo normal.
     - En **Windows 10**:
       a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.

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

c. Encuentre **Bitdefender Antivirus Plus** y seleccione **Desinstalar**.

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

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

f. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

g. Reinicie su sistema en modo normal.

3. Reinicie su producto Bitdefender.

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

  Para resolver esto:

  1. Reinicie su sistema e inicie en Modo Seguro. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 72).
  2. Elimine las otras soluciones de seguridad de su sistema:
     - En **Windows 7**:
       a. Haga clic en **Inicio**, vaya a **Panel Control** y doble clic en **Programas y Características**.
       b. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
       c. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.
     - En **Windows 8 y Windows 8.1**:
       a. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
       b. Haga clic en **Desinstalar un programa** o **Programas y características**.
       c. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
       d. Espere a que finalice el proceso de desinstalación y, luego, reinicie su sistema.

- En **Windows 10**:
  a. Haga clic en **Inicio** y, a continuación, haga clic en Configuración.
  b. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
  c. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  d. Espere a que finalice 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 e inicie en Modo Seguro. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 72).
2. Utilice la opción Restaurar sistema de Windows para restaurar el equipo a un punto anterior antes de la instalación del producto Bitdefender.
3. Reinicie el sistema de modo normal y contacte con nuestros represetantes de soporte para conseguir ayuda según se describe en la sección "*Pedir ayuda*" (p. 176).

27. 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.

- "*Bitdefender Modo de Rescate (Entorno de rescate en Windows 10)*" (p. 165)
- "*¿Qué hacer cuando Bitdefender encuentra amenazas en su equipo?*" (p. 169)
- "*¿Cómo limpio una amenaza de un archivo?*" (p. 170)
- "*¿Cómo limpio una amenaza de un archivo de correo electrónico?*" (p. 171)
- "*¿Qué hacer si sospecho que un archivo es peligroso?*" (p. 173)
- "*¿Qué son los archivos protegidos con contraseña del registro de análisis?*" (p. 173)
- "*¿Qué son los elementos omitidos en el registro de análisis?*" (p. 174)
- "*¿Qué son los archivos sobre-comprimidos en el registro de análisis?*" (p. 174)
- "*¿Por qué eliminó Bitdefender automáticamente un archivo infectado?*" (p. 174)

Si no puede encontrar su problema aquí, o si las soluciones presentadas no lo resuelven, puede contactar con los representantes de servicio técnico de Bitdefender como se presenta en el capítulo "*Pedir ayuda*" (p. 176).

27.1. Bitdefender Modo de Rescate (Entorno de rescate en Windows 10)

El **modo 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.

Una vez que Bitdefender Antivirus Plus está instalado en **Windows 7, Windows 8 y Windows 8.1** y que se ha descargado el archivo de imagen de rescate de Bitdefender, puede utilizar el modo Rescate incluso si no es capaz de arrancar en Windows.

En Windows 10, el Entorno de rescate de Bitdefender está integrado con Windows RE, por lo que no es necesario descargar ninguna imagen del modo Rescate en este sistema operativo.

Descarga de la imagen del modo Rescate de Bitdefender

Para poder utilizar el modo Rescate en **Windows 7, Windows 8 y Windows 8.1**, primero tiene que descargar su archivo de imagen de la siguiente manera:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Modo Rescate**.
3. Haga clic en **Sí** en la ventana de confirmación que aparece para reiniciar su equipo.

   Espere a que se descargue el archivo de imagen del modo Rescate de Bitdefender desde los servidores de Bitdefender. El equipo se reiniciará en cuanto finalice el proceso de descarga.

   Aparece un menú que le pide que seleccione un sistema operativo. En esta fase, puede optar por iniciar su sistema en modo Rescate o de la forma normal.

> **Nota**
> Debido a la integración con el entorno de recuperación de Windows en **Windows 10**, no es necesario descargar ninguna imagen del modo Rescate en este sistema operativo.

Arranque del sistema en modo Rescate en Windows 7, Windows 8 y Windows 8.1

Puede acceder al Modo Rescate de dos maneras:

Desde la interfaz de Bitdefender

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Modo Rescate**.
3. Haga clic en **Sí** en la ventana de confirmación que aparece para reiniciar su equipo.

4. Una vez que reinicie su equipo, aparecerá un menú que le pedirá que seleccione un sistema operativo. Elija **Modo rescate Bitdefender** para arrancar en un entorno de Bitdefender desde el cual podrá limpiar la partición de Windows.
5. Si se le solicita, pulse **Intro** y seleccione la resolución de pantalla más cercana a la que usa normalmente. A continuación, pulse de nuevo **Intro**.

   El modo Rescate de Bitdefender se cargará en unos momentos.

Inicie su equipo directamente desde el modo Rescate.

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

- En **Windows 7**:
  1. Pulse la tecla **F8** hasta que aparezca la pantalla **Opciones de arranque avanzadas**.
  2. Utilice las teclas de las flechas para seleccionar el modo Rescate de Bitdefender y, a continuación, pulse **Intro**.

     El modo Rescate de Bitdefender se cargará en unos momentos.
- En **Windows 8 y Windows 8.1**:
  1. Pulse la tecla **Mayúsculas** hasta que aparezca la pantalla **Opciones de arranque avanzadas**.
  2. Seleccione la opción **Utilizar otro sistema operativo** y, a continuación, Modo Rescate de Bitdefender.

     El modo Rescate de Bitdefender se cargará en unos momentos.

> **Nota**
> Solo es posible cargar su equipo en modo Rescate si ha descargado previamente el archivo de imagen del modo Rescate tal como se describe en "Descarga de la imagen del modo Rescate de Bitdefender" (p. 166).

Inicio del sistema en el Entorno de rescate de Windows 10

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

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. En el panel **ANTIVIRUS**, haga clic en **Entorno de rescate**.
3. Haga clic en **REINICIAR** en la ventana que aparece.

   El Entorno de rescate de Bitdefender se cargará en unos instantes.

Análisis del sistema en el modo Rescate (Entorno de rescate de Windows 10)

Para analizar su sistema en modo Rescate (Entorno de rescate):

- En **Windows 7, Windows 8 y Windows 8.1**:

  1. Acceda al Modo Rescate, como se describe en "Arranque del sistema en modo Rescate en Windows 7, Windows 8 y Windows 8.1" (p. 166).
  2. El logotipo de Bitdefender aparecerá y se empezarán a copiar los motores de la solución de seguridad.
  3. Aparecerá una ventana de bienvenida. Haga clic en **Continuar**.
  4. Se ha iniciado una actualización de la base de datos de información de amenazas.
  5. Tras completarse la actualización, aparecerá la ventana del Análisis antivirus bajo demanda de Bitdefender.
  6. Haga clic en **Analizar**, seleccione el objeto de análisis en la ventana que aparece y haga clic en **Abrir** para iniciar el análisis.

     Se recomienda analizar toda su partición de Windows.

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

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

- En **Windows 10**:

  1. Acceda al Entorno de rescate, según se describe en "Inicio del sistema en el Entorno de rescate de Windows 10" (p. 167).
  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.

27.2. ¿Qué hacer cuando Bitdefender encuentra amenazas en su equipo?

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

- Ha analizado su equipo 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 equipo.

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).

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

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

El primer método puede ser utilizado en modo normal:

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

a. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.

b. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.

c. En la ventana **Escudo**, desactive **Escudo de Bitdefender**.

2. Muestra los objetos ocultos en Windows. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo mostrar los objetos ocultos en Windows?*" (p. 70).
3. Busque la ubicación del archivo infectado (compruebe el log de análisis) y elimínelo.
4. Active la protección antivirus en tiempo real de Bitdefender.

En caso de que el primer método no lograse eliminar la infección:

1. Reinicie su sistema e inicie en Modo Seguro. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo reiniciar en Modo Seguro?*" (p. 72).
2. Muestra los objetos ocultos en Windows. Para averiguar cómo hacerlo, consulte "*¿Cómo puedo mostrar los objetos ocultos en Windows?*" (p. 70).
3. Busque la ubicación del archivo infectado (compruebe el log de análisis) y elimínelo.
4. Reiniciar su sistema e iniciar en modo normal.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 176).

27.3. ¿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. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
   b. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
   c. En la ventana **Escudo**, desactive **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 le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 176).

27.4. ¿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. Analizar la base de datos de correo con Bitdefender.
2. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
   b. En el panel **ANTIVIRUS**, haga clic en **Ajustes**.
   c. En la ventana **Escudo**, desactive **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 Administración de Datos de Archivo. Seleccione los archivos (.pst) de las carpetas personales para intentar compactar, y haga clic en Configuración. Haga clic en Compactar agora.
   - En Microsoft Outlook 2010/2013/2016: 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 agora.
6. Active la protección antivirus en tiempo real de Bitdefender.

Si esta información no le ayuda, puede contactar con el Soporte de Bitdefender como se describe en la sección "*Pedir ayuda*" (p. 176).

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

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

Para asegurarse de que su sistema está protegido:

1. Ejecute un **Análisis del sistema** con Bitdefender. Para averiguar cómo hacerlo, consulte "*¿Cómo analizo mi sistema?*" (p. 56).
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 "*Pedir ayuda*" (p. 176).

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

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

Por lo general, los elementos protegidos con contraseña son:

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

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

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

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

27.7. ¿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.

27.8. ¿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.

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

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

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.

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.

CONTACTO

28. PEDIR AYUDA

Bitdefender proporciona a sus clientes un nivel sin igual de soporte rápido y preciso. Si está experimentando cualquier incidencia o si tiene cualquier pregunta sobre su producto Bitdefender, puede utilizar varios recursos online para encontrar rápidamente una solución una respuesta. Al mismo tiempo, puede contactar con el equipo de Atención al Cliente de Bitdefender. Nuestro soporte responderá a todas sus preguntas en un corto periodo y le proporcionarán la asistencia que necesite.

La sección "*Resolución de incidencias comunes*" (p. 152) le proporciona la información necesaria sobre las incidencias más frecuentes a las que se pueda enfrentar cuando utiliza este producto.

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

- "Póngase en contacto con nosotros directamente desde Bitdefender Antivirus Plus" (p. 176)
- "Póngase en contacto con nosotros a través de nuestro Centro de Soporte online" (p. 177)

Póngase en contacto con nosotros directamente desde Bitdefender Antivirus Plus

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

Siga estos pasos:

1. Haga clic en **Soporte** en el menú de navegación de la interfaz de Bitdefender.
2. Dispone de las opciones siguientes:
   - **GUÍA DE USUARIO**

     Acceda a nuestra base de datos y busque la información necesaria.
   - **SOPORTE TÉCNICO**

     Acceda a nuestros vídeos tutoriales y artículos online.
   - **CONTACTAR SOPORTE**

Haga clic en **CONTACTAR CON SOPORTE** para iniciar la Herramienta de soporte de Bitdefender y contactar con el departamento de atención al cliente.

a. Rellene el formulario de envío con los datos necesarios:
   i. Seleccione el tipo de problema que ha experimentado.
   ii. Escriba una descripción del problema que se ha encontrado.
   iii. Haga clic en **TRATAR DE REPRODUCIR ESTE PROBLEMA** en caso de que se enfrente a un problema con el producto. Reproduzca el problema y luego haga clic en **FINALIZAR** en la zona REPRODUCIENDO EL PROBLEMA.
   iv. Haga clic en **CONFIRMAR TICKET**.
b. Siga rellenando el formulario de envío con los datos necesarios:
   i. Escriba su nombre completo.
   ii. Escriba su dirección de correo electrónico.
   iii. Marque la casilla de verificación de aceptación.
   iv. Haga clic en **CREAR PAQUETE DE DEPURACIÓN**.

   Espere unos momentos mientras Bitdefender recopila información relacionada con el producto. Esta información ayudará a nuestros ingenieros a encontrar una solución a su problema.
c. Haga clic en **CERRAR** para salir del asistente. Uno de nuestros representantes se pondrá en contacto con usted lo antes posible.

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

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

1. Visite https://www.bitdefender.com/support/consumer.html.

   El Centro de Soporte de Bitdefender alberga numerosos artículos que contienen soluciones de incidencias relacionadas con Bitdefender.
2. Utilice la barra de búsqueda en la parte superior de la ventana para encontrar los artículos que puedan proporcionar una solución a su

problema. Para hacer una búsqueda, simplemente escriba un término en la barra de Búsqueda y haga clic en **Buscar**.

3. Consulte los artículos o documentos relevantes e intente las soluciones propuestas.
4. Si la solución propuesta no resolviese el problema, acceda a

   https://www.bitdefender.com/support/contact-us.htmly póngase en contacto con nuestros representantes de soporte.

29. RECURSOS ONLINE

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

- Centro de soporte de Bitdefender:

  https://www.bitdefender.com/support/consumer.html

- Foro de Soporte de Bitdefender:

  https://forum.bitdefender.com

- El portal de seguridad informática HOTforSecurity:

  https://www.hotforsecurity.com

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

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

El Centro de soporte Bitdefender está siempre disponible en

https://www.bitdefender.com/support/consumer.html.

29.2. Foro de Soporte de Bitdefender

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

Si su producto de Bitdefender no funciona bien, si no puede eliminar determinadas amenazas de su equipo o si tiene preguntas sobre cómo funciona, publique en el foro su problema o pregunta.

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

Antes de publicar su problema o pregunta, busque en el foro un tema similar o que tenga relación.

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

29.3. Portal HOTforSecurity

El portal HOTforSecurity es una preciada fuente de información de seguridad informática. Aquí puede saber las varias amenazas a las que está expuesto su pc cuando está conectado a Internet (malware, phishing, spam, cibercriminales).

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

La página Web de HOTforSecurity es https://www.hotforsecurity.com.

30. INFORMACIÓN DE CONTACTO

La eficiente comunicación es la clave para un negocio con éxito. Desde 2001, BITDEFENDER se ha forjado una reputación incuestionable de lucha constante para mejorar la comunicación y así aumentar las expectativas de nuestros clientes y partners. Por favor no dude en contactar con nosotros.

30.1. Direcciones Web

Departamento Comercial: comercial@bitdefender.es
Centro de soporte:https://www.bitdefender.com/support/consumer.html
Documentación: documentation@bitdefender.com
Distribuidores Locales:https://www.bitdefender.com/partners
Programa de partners: partners@bitdefender.com
Relaciones con los medios: pr@bitdefender.com
Empleos: jobs@bitdefender.com
Envió de amenazas: virus_submission@bitdefender.com
Envíos de spam: spam_submission@bitdefender.com
Notificar abuso: abuse@bitdefender.com
Página Web:https://www.bitdefender.com

30.2. Distribuidores locales

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

Para encontrar un distribuidor de Bitdefender en su país:

1. Visite https://www.bitdefender.es/partners/partner-locator.html.
2. Elija su país y ciudad mediante las opciones correspondientes.
3. Si no encuentra un distribuidor Bitdefender en su país, no dude en contactar con nosotros por correo en comercial@bitdefender.es. Escriba su correo en inglés para que podamos ayudarle rápidamente.

30.3. Oficinas de Bitdefender

Las oficinas de Bitdefender están lista para responder a cualquier pregunta sobre sus áreas de operación, tanto comerciales como de asuntos generales. Sus direcciones y contactos están listados a continuación.

U.S.A

Bitdefender, LLC
6301 NW 5th Way, Suite 4300
Fort Lauderdale, Florida 33309
Tel (oficina&comercial): 1-954-776-6262
Comercial: sales@bitdefender.com
Soporte Técnico: https://www.bitdefender.com/support/consumer.html
Web: https://www.bitdefender.com

Reino Unido e Irlanda

BITDEFENDER LTD
C/O Howsons Winton House, Stoke Road, Stoke on Trent
Staffordshire, United Kindon, ST4 2RW
Correo: info@bitdefender.co.uk
Teléfono: (+44) 2036 080 456
Comercial: sales@bitdefender.co.uk
Soporte Técnico: https://www.bitdefender.co.uk/support/
Web: https://www.bitdefender.co.uk

Alemania

Bitdefender GmbH
TechnoPark Schwerte
Lohbachstrasse 12
D - 58239 Schwerte
Oficina: +49 2304 9 45 - 162
Fax: +49 2304 9 45 - 169
Comercial: vertrieb@bitdefender.de
Soporte Técnico: https://www.bitdefender.de/support/consumer.html
Web: https://www.bitdefender.de

Dinamarca

Bitdefender APS
Agern Alle 24, 2970 Hørsholm, Denmark
Oficina: +45 7020 2282
Soporte Técnico: http://bitdefender-antivirus.dk/
Web: http://bitdefender-antivirus.dk/

España

Bitdefender España, S.L.U.
C/Bailén, 7, 3-D
08010 Barcelona
Fax: +34 93 217 91 28
Teléfono: +34 902 19 07 65
Comercial: comercial@bitdefender.es
Soporte Técnico: https://www.bitdefender.es/support/consumer.html
Página Web: https://www.bitdefender.es

Rumania

BITDEFENDER SRL
Orhideea Towers Building, 15A Orhideelor Street, 11th fllor, district 6
Bucharest
Fax: +40 21 2641799
Teléfono comercial: +40 21 2063470
Correo comercial: sales@bitdefender.ro
Soporte Técnico: https://www.bitdefender.ro/support/consumer.html
Página Web: https://www.bitdefender.ro

Emiratos Árabes Unidos

Dubai Internet City
Building 17, Office # 160
Dubai, UAE
Teléfono comercial: 00971-4-4588935 / 00971-4-4589186
Correo comercial: mena-sales@bitdefender.com
Soporte Técnico: https://www.bitdefender.com/support/consumer.html
Página Web: https://www.bitdefender.com

Glosario

ActiveX

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

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

Actualización de información de amenazas

El patrón binario de una amenaza, utilizado por la solución de seguridad para detectarla y eliminarla.

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.

Adware

El adware habitualmente se combina con aplicaciones que son gratuitas a cambio de que el usuario acepte la instalación del componente adware. Puesto que las aplicaciones adware generalmente se instalan una vez el usuario acepta los términos de licencia que manifiestan el propósito de la aplicación, no se comete ningún delito.

Sin embargo, los pop-up de publicidad pueden resultar molestos, y en algunos casos afectar al rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas

de privacidad a aquellos usuarios que no eran plenamente conscientes de los términos de la licencia.

Amenaza

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.

Amenaza persistente avanzada

Una amenaza persistente avanzada (Advanced Persistent Threat, APT) explota vulnerabilidades de los sistemas para robar información importante que se entrega a la fuente. Grandes grupos, como organizaciones, empresas o gobiernos, son el objetivo primordial de esta amenaza.

El objetivo de una amenaza persistente avanzada es pasar desapercibida durante mucho tiempo, para poder monitorizar y recopilar información importante sin dañar las máquinas objetivo. El método empleado para inyectar la amenaza en la red es un archivo PDF o un documento de Office que parezca inofensivo, para que cualquier usuario decida ejecutarlo.

Applet de Java

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

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

Archivo Comprimido

Disco, cinta o directorio conteniendo ficheros almacenados.

Fichero conteniendo uno o varios ficheros en formato comprimido.

Archivo de informe

Es un fichero que lista las acciones ocurridas. Bitdefender mantiene un archivo de informe que incluye la ruta analizada, las carpetas, el número de archivos comprimidos y no comprimidos analizados, así como cuántos archivos infectados o sospechosos se encontraron.

Área de notificación del Sistema

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

Ataque de diccionario

Los ataques de adivinación de contraseñas se utilizan para entrar en un sistema informático introduciendo una combinación de palabras habituales para generar potenciales contraseñas. El mismo método se emplea para adivinar claves de descifrado de mensajes o documentos encriptados. Los ataques de diccionario tienen éxito porque mucha gente suele elegir contraseñas con palabras cortas y sencillas que son fáciles de adivinar.

Ataque de fuerza bruta

El ataque de adivinación de contraseñas se utiliza para entrar en un sistema informático introduciendo posibles combinaciones de contraseñas, principalmente a partir de las más fáciles de adivinar.

Backdoor

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

Botnet

El término "botnet" se compone de las palabras "robot" y "network" (red). Los botnets son dispositivos conectados a Internet e infectados con amenazas y se pueden utilizar para enviar correos electrónicos no deseados, robar datos, controlar remotamente dispositivos vulnerables o propagar spyware, ransomware y otros tipos de amenazas. Su objetivo es infectar el máximo de dispositivos conectados posible, como PC, servidores, y dispositivos móviles o de IoT pertenecientes a grandes empresas o industrias.

Ciberacoso

Cuando compañeros o extraños abusan de los niños con el ánimo de lastimarles físicamente. Para causar daños emocionales, los agresores les envían mensajes ofensivos o fotos desagradables, lo que provoca que sus víctimas se aíslen de los demás o sientan una gran frustración.

Cliente de mail

Un cliente de correo es una aplicación que permite enviar y recibir correo electrónico.

Código de activación

Es una clave única que se puede comprar al por menor y se utiliza para activar un producto o servicio determinado. Un código de activación permite la activación de una suscripción válida durante un cierto período de tiempo y para determinado número de dispositivos, y también puede utilizarse para ampliar una suscripción con la condición de que se genere para el mismo producto o servicio.

Cookie

En la industria del Internet, las cookies se describen como pequeños ficheros conteniendo información sobre los ordenadores individuales que se pueden analizar y usar por los publicistas para determinar los intereses y los gustos online de los usuarios respectivos. En este ambiente, la tecnología de las cookies se desarrolla con la intención de construir reclamos y mensajes publicitarios correspondientes a los intereses declarados por usted. Es un arma de doble filo para mucha gente porque, por un lado, es más eficiente y pertinente que usted vea publicidades relacionadas con sus intereses. Por otro lado, implica seguir cada paso suyo y cada clic que usted haga. Por consiguiente, es normal que haya resultado un debate sobre la privacidad y mucha gente se

sintió ofendida por la idea de ser vista como "número de SKU" (el código de barras ubicado en la parte posterior de los paquetes analizados a la salida de los supermercados). Aunque esta perspectiva pueda parecer extremista, en algunos casos es cierta.

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

Depredadores online
Personas que buscan conversar con menores o adolescentes con el fin de implicarles en actividades sexuales ilegales. Las redes sociales son el lugar ideal donde los niños vulnerables pueden ser fácilmente contactados y convencidos para que realicen actividades sexuales, ya sea online o en persona.

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

Elementos en 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.

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

Exploits
Una forma de aprovechar los diferentes errores o vulnerabilidades presentes en un equipo (software o hardware). Así, los piratas informáticos pueden tomar el control de equipos o redes.

Explorador

Abreviatura de navegador web, una aplicación de software utilizada para localizar y mostrar páginas web. los navegadores más populares incluyen Microsoft Internet Explorer, Mozilla Firefox y Google Chrome. Estos son navegadores gráficos, lo cual significa que pueden mostrar tanto gráficos como textos. Además, la mayoría de los navegadores modernos pueden mostrar información multimedia: sonido e imágenes, aunque requieren plugins para ciertos formatos.

Extensión de un archivo

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

Muchos sistemas operativos utilizan extensiones de nombres de archivo, por ejemplo, Unix, VMS y MS-DOS. Normalmente son de una a tres letras (algunos viejos SO no soportan más de tres). Por ejemplo "c" para código fuente C, "ps" para PostScript, o "txt" para texto plano.

Falso positivo

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

Gusano

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

Heurístico

Un método basado en reglas para identificar nuevas amenazas. Este método de análisis no se basa en una determinada base de datos de información de amenazas. La ventaja de un análisis heurístico es que no le engaña una nueva variante de una amenaza existente. Sin embargo, puede que informe ocasionalmente de códigos sospechosos en programas normales, generando el llamado "falso positivo".

Honeypot (sistema trampa)

Un sistema informático que sirve como señuelo para atraer a los piratas informáticos con el fin de estudiar cómo actúan e identificar los métodos delictivos que utilizan para recabar información del sistema. Las empresas y grandes corporaciones están más interesadas ??en implementar y utilizar estos sistemas trampa para mejorar su estado general de seguridad.

IP

Internet Protocol - Protocolo enrutable dentro del protocolo TCP/IP y que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reensamblado de los paquetes IP.

Keylogger

Un keylogger es una app que registra todo lo que usted escribe.

Los keyloggers en su esencia no son maliciosos. Pueden ser utilizados para propósitos legítimos, como monitorizar la actividad de los empleados o niños. Sin embargo, son cada vez más utilizados por cibercriminales con fines maliciosos (por ejemplo, para recoger datos privados, como credenciales y números de seguridad social).

Línea de comando

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

Memoria

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

No Heurístico

Este método de análisis se basa en una determinada base de datos de información de amenazas. La ventaja del análisis no heurístico es que no se deja engañar por lo que podría parecer una amenaza y no genera falsas alarmas.

Phishing

El acto de enviar un email a un usuario simulando pertenecer a una empresa legítima e intentar estafar al usuario solicitándole información privada que después se utilizará para realizar el robo de identidad. El email conduce al usuario a visitar una página web en la que se le solicita actualizar información personal, como contraseñas y números de tarjetas de crédito, de la seguridad social y números de cuentas corrientes, que en realidad ya posee la organización auténtica. La página web, en cambio,

es una réplica fraudulenta, creada sólo para robar la información de los usuarios.

Photon

Photon es una innovadora tecnología no intrusiva de Bitdefender, diseñada para minimizar el impacto de la solución de seguridad en el rendimiento. Monitorizando en segundo plano la actividad de su PC, crea patrones de uso que ayudan a optimizar los procesos de arranque y de análisis.

Programas Empaquetados

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

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

Puerto

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

En las redes de tipo TCP/IP y UDP representa el 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.

Red Privada Virtual (VPN)

Es una tecnología que permite una conexión directa temporal y cifrada a una determinada red a través de una red menos segura. De esta forma, el envío y recepción de datos está cifrado y es seguro, lo que dificulta su intercepción por parte de los fisgones. Una muestra de seguridad es la autenticación, que solo se puede lograr utilizando un nombre de usuario y contraseña.

Rootkit

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

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

Rootkits no son de naturaleza mala. Por ejemplo, los sistemas y algunas aplicaciones esconden ficheros críticos usando rootkits. 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.

Ruta

Las rutas exactas de un archivo en un equipo. Esta suma de información es una ruta completamente válida.

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

Script

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

Sector de arranque

Un sector al principio de cada disco y que identifica la arquitectura del disco (tamaño del sector, tamaño del cluster, etc). Para los discos de inicio, el sector de arranque también incluye un programa para cargar el sistema operativo.

Spam

Correo basura o los posts basura en los grupos de noticias. Se conoce generalmente como correo no solicitado.

Spyware

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

Suscripción

Acuerdo de compra que otorga al usuario el derecho a utilizar un producto o servicio determinado en un número concreto de dispositivos y durante cierto periodo de tiempo. Una suscripción caducada puede renovarse automáticamente utilizando la información proporcionada por el usuario en su primera compra.

TCP/IP

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

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los 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 viene de la historia de la Ilíada de Homero, en la cual Grecia entrega un caballo gigante hecho de madera a sus enemigos, los Troyanos, supuestamente como oferta de paz. Pero después de que los troyanos arrastraran el caballo dentro de las murallas de su ciudad, los soldados griegos salieron del vientre hueco del caballo y abrieron las puertas de la ciudad, permitiendo a sus compatriotas entrar y capturar Troya.

Unidad de disco

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

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

Una unidad de disquetera abre disquetes.

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

Virus de boot

Una amenaza que infecta el sector de arranque de un disco fijo o disquete. Un intento de arranque desde un disquete infectado con un

virus en el 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.

Virus de macro

Un tipo de amenaza informática codificada como una macro incrustada en un documento. Muchas aplicaciones, como Microsoft Word o Excel, soportan potentes lenguajes macro.

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

Virus Polimórfico

Una amenaza que cambia de forma con cada archivo que infecta. Como no tienen un patrón binario constante, estas amenazas son difíciles de identificar.