Bitdefender ANTIVIRUS FREE

GUÍA DE USUARIO

Bitdefender Antivirus Free

Guía de usuario

Fecha de publicación 12/04/2023

Aviso Legal

Bitdefender

Tabla de contenidos

ACERCA DE ESTA GUÍA

Propósito y público objetivo

Esta guía está dirigida a todos los usuarios de Windows que hayan elegido Bitdefender Antivirus Free como una solución de seguridad para sus computadoras. La información presentada en este libro es adecuada no solo para los que tienen conocimientos de informática, sino que es accesible para todos los que pueden trabajar con una PC con Windows.

Descubrirá cómo configurar y utilizar Bitdefender Antivirus Free para protegerse contra amenazas y otro software malicioso. Aprenderás a sacar el máximo partido a tu Bitdefender.

Le deseamos una conferencia agradable y útil.

Como usar esta guia

Esta guía está organizada en torno a varios temas principales:

Primeros pasos (página 14)

Comience con Bitdefender Free y su interfaz de usuario.

Gestión de su seguridad (página 44)

Aprenda a usar Bitdefender Free para protegerse contra software malicioso.

Cómo (página 70)

Obtenga más información sobre Bitdefender gratuito.

Obteniendo ayuda (página 110)

Dónde buscar y dónde pedir ayuda si aparece algo inesperado.

Convenciones utilizadas en esta guía

Convenciones tipográficas

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

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

Advertencias

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

Nota

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

Importante

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

Advertencia

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

Solicitud de comentarios

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

Háganos saber enviando un correo electrónico a documentation@bitdefender.com. Escriba todos sus correos electrónicos

relacionados con la documentación en inglés para que podamos procesarlos de manera eficiente.

1. PASOS DE LA INSTALACIÓN

1.1. Preparándose para la instalación

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

- Asegúrese de que el dispositivo donde piensa instalar Bitdefender cumple los requisitos del sistema. Si el dispositivo no cumple con todos los requisitos del sistema, Bitdefender no se instalará o, si estuviera instalado, no funcionaría correctamente y provocaría demoras e inestabilidad en el sistema. Para ver una lista completa de los requisitos del sistema, consulte Requisitos del sistema (página 4).
- Inicie sesión en el dispositivo utilizando una cuenta de Administrador.
- Desinstale cualquier otro software similar del dispositivo. Si se detectase alguno durante el proceso de instalación de Bitdefender, se le notificará para que lo desinstale. La ejecución de dos programas de seguridad simultáneamente puede afectar al funcionamiento y causar mayores problemas con el sistema. Windows Defender se desactivará durante la instalación.
- Desactive o elimine cualquier programa cortafuego que puede estar ejecutándose en el dispositivo. La ejecución de dos programas de cortafuego simultáneamente puede afectar al funcionamiento y causar mayores problemas con el sistema. Windows Firewall se desactivará durante la instalación.
- Durante la instalación, se recomienda que su dispositivo esté conectado a Internet, incluso si la realiza desde un CD o DVD. Si hay disponibles versiones más recientes de los archivos de la aplicación incluidos en el paquete de instalación, Bitdefender puede descargarlas e instalarlas.

1.2. Requisitos del sistema

Sólo podrá instalar Bitdefender Antivirus Free en aquellos dispositivos 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)
- 2 GB de memoria (RAM)

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

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

- En **Windows 7**, haga clic con el botón derecho sobre el icono **Mi PC** del Escritorio y seleccione la opción **Propiedades** del menú.
- En **Windows 8**, desde la pantalla de inicio de Windows, localice **Equipo** (por ejemplo, puede empezar escribiendo "Equipo" directamente en la pantalla Inicio) y, luego, haga clic con el botón derecho sobre su icono. En **Windows 8.1**, busque **Este PC**.
  Seleccione **Propiedades** en el menú inferior. Consulte el área del **sistema** para obtener información sobre el tipo de sistema.
- En **Windows 10**, escriba **Sistema** en el cuadro de búsqueda de la barra de tareas y haga clic en su icono. Consulte el área del **sistema** para obtener información sobre el tipo de sistema.

1.3. Requisitos de software

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

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

1.4. Instalando su producto Bitdefender

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

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

1.4.1. Instalación desde Bitdefender Central

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

Para descargar Bitdefender Antivirus Free desde Bitdefender Central:

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

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

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

Validación de la instalación

Bitdefender comprueba primero su sistema para validar la instalación.

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

Si se detecta una solución de seguridad incompatible o una versión anterior de Bitdefender, se le solicitará que la desinstale de su sistema. Por favor, siga las instrucciones para desinstalar el software de su sistema, evitando así posibles problemas que ocurran en un futuro. Es posible que deba reiniciar su dispositivo para completar la eliminación de las soluciones de seguridad detectadas.

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

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

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

Paso 1 - Instalación de Bitdefender

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

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

Pueden realizarse dos tareas adicionales en este paso:

- Mantenga habilitada la opción **Enviar informes del producto**. Permitiendo esta opción se envían informes con datos sobre cómo utiliza el producto a los servidores de Bitdefender. Esta información

es fundamental para depurar el producto y nos ayuda a ofrecerle una experiencia de usuario mejor en el futuro. Tenga en cuenta que estos informes no contienen datos confidenciales, como su nombre o dirección IP, y que no se utilizarán con fines comerciales.

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

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

Paso 2 - Instalación en curso

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

Paso 3 - Instalación completada

Su producto Bitdefender se ha instalado correctamente.

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

Paso 4 - Análisis del dispositivo

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

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

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

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

Paso 5 - Primeros pasos

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

Haga clic en **FINALIZAR** para acceder a la interfaz de Bitdefender Antivirus Free.

1.4.2. 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 {1}**Instalar desde CD/DVD**. En tal caso, se instalará el producto Bitdefender disponible en el disco y se descargará una versión más reciente de los servidores de Bitdefender mediante la actualización del producto.

Validación de la instalación

Bitdefender comprueba primero su sistema para validar la instalación.

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

Si se detecta una solución de seguridad incompatible o una versión anterior de Bitdefender, se le solicitará que la desinstale de su sistema. Por favor, siga las instrucciones para desinstalar el software de su sistema, evitando así posibles problemas que ocurran en un futuro. Es posible que deba reiniciar su dispositivo para completar la eliminación de las soluciones de seguridad detectadas.

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

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

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

Paso 1 - Instalación de Bitdefender

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

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

En este paso se pueden realizar dos tareas adicionales:

- Mantener el **Enviar informes de productos** opción habilitada. Al habilitar esta opción, los informes que contienen información sobre cómo usa el producto se envían a los servidores de Bitdefender. Esta información es esencial para mejorar el producto y puede ayudarnos a brindar una mejor experiencia en el futuro. Tenga en cuenta que estos informes no contienen datos confidenciales, como su nombre o dirección IP, y que no se utilizarán con fines comerciales.
- Seleccione el idioma en el que desea instalar el producto.

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

Paso 2 - Instalación en proceso

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

Paso 3 - Instalación completada

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

Paso 4: análisis del dispositivo

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

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

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

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

Paso 5 - Cuenta de Bitdefender

Tras completar la configuración inicial, aparece la ventana Bitdefender Account. Es necesaria una cuenta Bitdefender para poder activar el producto y utilizar sus características online. Para más información, diríjase a Bitdefender Central (página 31).

Proceder de acuerdo a su situación.

- **Quiero crear una cuenta de Bitdefender**

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

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

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

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

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

- **Quiero iniciar la sesión con mi cuenta de Microsoft, Facebook o Google**
  Para iniciar sesión con su cuenta de Microsoft, Facebook o Google:
  1. Seleccione el servicio que desee usar. Será redirigido a la página de inicio de sesión de ese servicio.
  2. Siga las instrucciones proporcionadas por el servicio seleccionado para vincular su cuenta a Bitdefender.

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

Paso 6 - Active su producto

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

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

Proceda de acuerdo con su situación:

- Tengo un código de activación
  En este caso, active el producto siguiendo estos pasos:

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

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

  2. **Quiero evaluar Bitdefender**
     En este caso, puede utilizar el producto durante un período de treinta días. Para iniciar el período de evaluación seleccione **No tengo ninguna suscripción; quiero probar el producto gratuitamente** y, a continuación, haga clic en **CONTINUAR**.

Paso 7 - Primeros pasos

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

Hacer clic **FINALIZAR** para acceder a la Bitdefender Antivirus Free interfaz.

2. PRIMEROS PASOS

2.1. Fundamentos

Una vez que haya instalado Bitdefender Antivirus Free, su dispositivo estará protegido contra todo tipo de amenazas (como malware, spyware, ransomware, exploits, botnets y troyanos) y amenazas de Internet (como piratas informáticos, phishing y spam).

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.

Protección de cámaras web mantiene a raya las apps que no son de fiar para que no accedan a su cámara de vídeo, con lo que evita cualquier intento de ataque por parte de piratas informáticos. El acceso de las apps populares a su cámara web se permitirá o no según las opciones escogidas por los usuarios de Bitdefender.

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.

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.

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 (página 16).

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 (página 40).

De vez en cuando, debería abrir Bitdefender y corregir cualquier problema que haya. Puede que tenga que configurar componentes específicos de Bitdefender o adoptar medidas preventivas para proteger su dispositivo y sus datos.

Para usar las opciones online de Bitdefender Antivirus Free y administrar sus suscripciones y dispositivos, acceda a su cuenta Bitdefender. Para más información, diríjase a Bitdefender Central (página 31).

En la sección Cómo (página 70) hallará instrucciones paso a paso de cómo realizar tareas comunes. Si tiene algún problema mientras utiliza Bitdefender, consulte la sección Resolución de incidencias comunes (página 91), donde hallará soluciones para la mayoría de los problemas más habituales.

2.1.1. Notificaciones

Bitdefender mantiene un registro detallado de los eventos relacionados con la actividad en su dispositivo. Siempre que ocurra algo relevante para la seguridad de su sistema o de sus datos, se añadirá un nuevo mensaje al área de Notificaciones de Bitdefender, como si fuera un nuevo mensaje de correo electrónico que apareciese en su bandeja de entrada.

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

Para acceder al registro de **notificaciones**, haga clic en Notificaciones en el menú de navegación de la interfaz de **Bitdefender**. Cada vez que se produce un evento crítico, se puede ver un contador en el icono .

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

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

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

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

2.1.2. Perfiles

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

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

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

Perfil de Trabajo

Optimiza la eficiencia en su trabajo identificando y adaptando los ajustes del producto y del sistema.

Perfil de Películas

Mejora los efectos visuales y elimina las interrupciones cuando se ven películas.

Perfil de Juego

Mejora los efectos visuales y elimina las interrupciones cuando se juega.

Perfil de redes Wi-Fi públicas

Aplica los ajustes del producto para beneficiarse de una protección completa mientras está conectado a una red inalámbrica no segura.

Perfil del modo Batería

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

Configurar la activación automática de perfiles

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

La primera vez que acceda a los **Perfiles** se le pedirá que active los perfiles automáticos. Para ello, puede simplemente hacer clic en **ACTIVAR** en la ventana que aparece.

Puede hacer clic en **AHORA NO** si desea activar esta característica más adelante.

Para permitir que Bitdefender active los perfiles automáticamente:

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

2.1.3. Configuración de protección por contraseña de Bitdefender

Si no es la única persona con derechos administrativos que utiliza este dispositivo, se recomienda que proteja sus ajustes 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. Hacer clic **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.

2.1.4. 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. Hacer clic **Ajustes** en el menú de navegación de la Interfaz de Bitdefender.
2. Seleccione la pestaña **Avanzado**.
3. Desactive los **Informes del producto**.

2.1.5. 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. Hacer clic **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.

2.2. Interfaz de Bitdefender

Bitdefender Antivirus Free 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 al área de ajustes, a las notificaciones y a las **secciones de Bitdefender** para realizar una configuración detallada y tareas administrativas avanzadas.

Desde la parte superior de la interfaz principal, puede acceder a su **cuenta de Bitdefender**. Además, puede ponerse en contacto con nosotros para obtener ayuda en caso de tener alguna pregunta o si sucede algo inesperado.

2.2.1. Icono del área de notificación

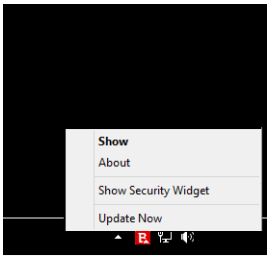
Para administrar todo el producto con mayor rapidez, puede recurrir al icono de Bitdefender en la bandeja del sistema.

Nota
Puede que el icono de Bitdefender no esté siempre visible. Para que el icono se muestre de forma permanente:

- En **Windows 7, Windows 8 y Windows 8.1**
  1. Haga clic en la flecha de 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 a **Agente de Bitdefender**.

Si hace doble clic en este icono se abrirá la interfaz de BitDefender. Si hace clic derecho sobre el icono, aparecerá un menú contextual desde el que podrá administrar rápidamente el producto BitDefender.

- **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.
- **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 dispositivo o como funciona el producto, mostrando un símbolo especial, como el siguiente:

No hay ninguna incidencia que afecte a la seguridad de su sistema.

Las incidencias críticas afectan a la seguridad de su sistema. Requieren su atención inmediata y han de solucionarse lo antes posible.

Si Bitdefender no funciona, el icono del área de notificación aparecerá en un fondo gris: . Esto suele suceder al caducar la suscripción. También puede ocurrir si los servicios de Bitdefender no responden o cuando algún otro error afecta al funcionamiento normal de Bitdefender.

2.2.2. 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, realizar acciones rápidas e instalar Bitdefender en otros dispositivos.
- **Protección**. Desde aquí puede lanzar y configurar análisis antivirus, acceder a los ajustes del cortafuego, 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, abrir la aplicación de VPN y proteger a sus hijos monitorizando y restringiendo su actividad online.
- **Utilidades**. Desde aquí, puede mejorar la velocidad del sistema y configurar la característica Antirrobo para sus dispositivos.
- **Notificaciones**. Desde aquí tiene acceso a las notificaciones generadas.
- **Ajustes**. Desde aquí tiene acceso a los ajustes generales.

- **Soporte técnico**. Desde aquí, siempre que necesite ayuda para resolver cualquier incidencia con su Bitdefender Antivirus Free, puede ponerse en contacto con el servicio de soporte técnico de Bitdefender.
- **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.

2.2.3. 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 dispositivo.

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 y funcionando a la velocidad óptima. También puede instalar Bitdefender en otros dispositivos, siempre y cuando su suscripción tenga suficientes puestos disponibles.

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 dispositivo 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 dispositivo, 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.

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. Hacer clic **Ajustes** en el menú de navegación de la Interfaz de Bitdefender.
2. En la ventana **General**, desactive las **Notificaciones de recomendación**.

Acciones rápidas

Mediante acciones rápidas, puede iniciar rápidamente tareas que considere importantes para mantener su sistema protegido y funcionando a una velocidad óptima.

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:

- **Quick Scan**. Ejecute un análisis rápido para detectar de inmediato las posibles amenazas que puedan existir en su dispositivo.
- **Análisis del sistema**. Ejecute un análisis del sistema para asegurarse de que su dispositivo está libre de amenazas.
- **Análisis de vulnerabilidades**. Analice su dispositivo en busca de vulnerabilidades para asegurarse de que todas las aplicaciones instaladas, además del sistema operativo, están actualizadas y funcionan correctamente.
- **Asesor de seguridad Wi-Fi**. Abra la ventana del Asesor de seguridad Wi-Fi dentro del módulo de Vulnerabilidades.
- **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 dispositivo.
- **Abra el Optimizador en un clic**. Libere espacio en disco, corrija errores del registro y proteja su privacidad eliminando archivos que ya no le hacen falta con solo hacer clic en un botón.

Para empezar a proteger dispositivos adicionales con Bitdefender:

1. Haga clic en **Instalar en otro dispositivo**.
   Aparece una nueva ventana en la pantalla.
2. Toque **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 Free 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.

2.2.4. Las secciones de Bitdefender

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

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**
- **Utilidades**

Protección

En la sección de Protección puede configurar sus ajustes de seguridad avanzados, gestionar los amigos y los emisores de spam, ver y editar los ajustes de conexión de red, configurar las características de 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
- Entorno de rescate

Si desea obtener más información sobre las tareas de análisis y sobre cómo configurar la protección antivirus, consulte Protección Antivirus (página 44).

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 en línea (página 67).

CORTAFUEGO

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

Para obtener más información sobre la configuración del cortafuego, consulte Cortafuego.

ADVANCED THREAT DEFENSE

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 Defensa contra amenazas avanzadas (página 64).

ANTISPAM

La característica antispam de Bitdefender garantiza que su bandeja de entrada esté libre de correo electrónico no deseado mediante el filtrado del tráfico de correo POP3.

Para obtener más información sobre la protección antispam, consulte Antispam.

VULNERABILIDADES

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

las redes inalámbricas inseguras a las que se conecta. Haga clic en **Abrir** en el módulo de Vulnerabilidades para acceder a sus características.

La característica de **Análisis de vulnerabilidades** le permite 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 **Iniciar análisis** para realizar un análisis de su dispositivo.

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

Para obtener más información sobre la configuración de la protección contra vulnerabilidades, consulte Vulnerabilidad.

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.

Privacidad

En la sección de Privacidad puede abrir la aplicación Bitdefender VPN, cifrar sus datos privados, proteger sus transacciones online, mantener a salvo su cámara web y su experiencia de navegación, así como proteger a sus hijos monitorizando y restringiendo sus actividades en Internet.

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.

PROTECCIÓN DE VÍDEO Y AUDIO

La protección de vídeo y audio mantiene su cámara web a salvo al bloquear el acceso a ella por parte de aplicaciones que no sean de confianza y notificarle cuándo intentan acceder a su micrófono.

Para obtener más información sobre cómo mantener su cámara web protegida contra accesos no deseados y cómo configurar Bitdefender para notificarle sobre la actividad de su micrófono, consulte Protección de vídeo y audio.

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 la activación de Bitdefender Safepay™, consulte Seguridad Safepay para las transacciones online.

CONTROL PARENTAL

El Control parental de Bitdefender le permite monitorizar lo que hacen sus hijos en sus dispositivos. En caso de contenidos inapropiados, puede decidir restringir su acceso a Internet o a ciertas aplicaciones.

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

Para obtener más información sobre la configuración del Control parental, consulte Control parental.

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.

Utilidades

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

Optimizador en un clic

Bitdefender Total Security no solo ofrece seguridad, sino que también le ayuda a mantener el rendimiento de su dispositivo.

Nuestro Optimizador en un clic le ayudará a encontrar y eliminar los archivos innecesarios de su dispositivo en un solo paso.

Para obtener más información, consulte OneClick Optimizer.

Antirrobo

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

El Antirrobo de Bitdefender ofrece las siguientes características:

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

Para obtener más información sobre cómo puede evitar que su sistema caiga en malas manos, consulte .

Protección de datos

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

Para obtener más información al respecto, consulte Protección de datos.

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.

Para obtener más información sobre esta característica, consulte Perfiles.

2.2.5. Cambiar el idioma del producto

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

1. Hacer clic **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.

2.3. Bitdefender Central

2.3.1. Acerca de 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 iOS y Android.

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:

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

- Configure los ajustes del **Asesor parental** para los dispositivos de sus hijos y monitorice su actividad donde quiera que estén.

2.3.2. Acceso a Bitdefender Central

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

- Desde la interfaz principal de Bitdefender:
  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. Ir a: https://central.bitdefender.com
  3. Inicie sesión en su cuenta con su dirección de correo electrónico y contraseña.

- Desde su dispositivo Android o iOS:
  1. Abra la app Bitdefender Central que ha instalado.

> **Nota**
> En este material, hemos incluido las opciones que puede encontrar en la interfaz web.

2.3.3. 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. Acceso Centro de Bitdefender.
2. Toque el icono en la parte superior derecha de la pantalla.
3. Toque **Cuenta de Bitdefender** en el menú deslizante.
4. Seleccione la pestaña **Contraseña y seguridad**.
5. Haga clic en **Autenticación en dos fases**.
6. Toque **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.
        Toque **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 y escriba el código que se le proporciona.
     a. Haga clic en **USAR CORREO ELECTRÓNICO** para comenzar.

b. Lea su correo electrónico y escriba el código que se le proporciona.

c. Toque **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. Cada código puede utilizarse una sola 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.

2.3.4. 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. Acceso Centro de Bitdefender.
2. Haga clic en el icono en la parte superior derecha de la pantalla.
3. Hacer clic **Cuenta de Bitdefender** en el menú deslizante.
4. Selecciona el **contraseña y seguridad** pestaña.
5. Toque **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.

2.3.5. Actividad

En el área de Actividad, tiene acceso a información sobre los dispositivos que tienen Bitdefender instalado.

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

- **Mis dispositivos.** Aquí puede ver el número de dispositivos conectados junto con el estado de su protección. Para solucionar problemas de forma remota en los dispositivos detectados, toque **Solucionar problemas** y, a continuación, toque **ANALIZAR Y SOLUCIONAR LOS PROBLEMAS**.
  Para ver más información sobre los problemas detectados, haga clic en **Ver problemas**.
  La información sobre las amenazas detectadas no se puede recuperar de los dispositivos basados en iOS.
- **Amenazas bloqueadas.** Aquí puede ver un gráfico que muestra una estadística general con información sobre las amenazas bloqueadas durante las últimas 24 horas y siete días. La información mostrada se recupera dependiendo del comportamiento malicioso detectado en los archivos, aplicaciones y URL a los que se accede.
- **Principales usuarios con amenazas bloqueadas.** Aquí puede ver los usuarios que se han sido objeto de más amenazas.
- **Principales dispositivos con amenazas bloqueadas.** Aquí puede ver los dispositivos donde se han encontrado más amenazas.

2.3.6. Mis suscripciones

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

Compruebe las suscripciones disponibles

Para comprobar sus suscripciones disponibles:

1. Acceso Centro de Bitdefender.
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).

Activar la suscripción

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

Si ha comprado un código de activación a uno de nuestros resellers o lo ha recibido de regalo, puede añadir su disponibilidad a su suscripción de Bitdefender.

Para activar una suscripción mediante un código de activación, siga estos pasos:

1. Acceso Centro de Bitdefender.
2. Selecciona el **mis Suscripciónes** panel.
3. Haga clic en el botón **CÓDIGO DE ACTIVACIÓN** y, a continuación, escriba el código en el campo correspondiente.
4. Toque **ACTIVAR** para continuar.

La suscripción ya está activada.

Renovar suscripción

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

1. Acceso Centro de Bitdefender.
2. Selecciona el **mis Suscripciónes** panel.
3. Seleccione la tarjeta de suscripción deseada.
4. Toque **RENOVAR** para continuar.

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

2.3.7. Mis dispositivos

El área **Mis sispositivos** de su cuenta de Bitdefender le da la posibilidad de instalar, administrar y llevar a cabo acciones remotas en su producto de Bitdefender en cualquier dispositivo, siempre y cuando esté encendido y conectado a Internet. Las tarjetas de 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.

Añadir un nuevo dispositivo

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

1. Acceso Centro de Bitdefender.
2. Selecciona el **Mis dispositivos** panel y, a continuación, toque **INSTALAR PROTECCIÓN**.
3. Elija una de las dos opciones disponibles:
   - **Protege este dispositivo**
     Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, toque el botón correspondiente.
   - **Proteger otros dispositivos**
     Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, toque el botón correspondiente.
     Toque **ENVIAR ENLACE DE DESCARGA**. Introduzca una dirección de correo electrónico en el campo correspondiente y toque **ENVIAR CORREO**. 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 el que desea instalar su producto Bitdefender, verifique la cuenta de correo electrónico que ingresó y luego toque el botón de descarga correspondiente.
4. Espere a que finalice la descarga y, acto seguido, ejecute el instalador.

Personalice su dispositivo

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

1. Acceso Centro de Bitdefender.
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, toque **GUARDAR**.

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

1. Acceso Centro de Bitdefender.
2. Selecciona el **Mis dispositivos** panel.
3. Toque la tarjeta del dispositivo deseado, y luego el ⋮ icono en 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 incluyendo una foto, seleccionando una fecha de nacimiento y añadiendo una dirección de correo electrónico y un número de teléfono.
6. Haga clic en **AÑADIR** para guardar el perfil.
7. Seleccione el propietario deseado en la lista de **Propietarios de dispositivos** y, a continuación, toque **ASIGNAR**.

Acciones remotas

Para actualizar Bitdefender remotamente en un dispositivo:

1. Acceso Centro de Bitdefender.
2. Selecciona el **Mis dispositivos** panel.
3. Toque la tarjeta del dispositivo deseado, y luego el ⋮ icono en la esquina superior derecha de la pantalla.
4. Seleccione **Actualizar**.

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

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

- **Panel de control.** En esta ventana puede 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, toque la flecha desplegable en el área de estado superior para obtener más información. Desde aquí, puede
- **Protección.** Desde esta ventana puede ejecutar de forma remota un análisis rápido o un análisis del sistema en sus dispositivos. Toque 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.
- **Optimizador.** Aquí puede mejorar el rendimiento de un dispositivo de forma remota mediante un rápido análisis, detección y limpieza de archivos inútiles. Toque el botón **INICIAR** y, a continuación, seleccione las áreas que desea optimizar. Toque nuevamente en el botón **INICIAR** para poner en marcha el proceso de optimización. Toque **Más detalles** para acceder a un informe pormenorizado acerca de los problemas solucionados.
- **Antirrobo.** Si no se acuerda de dónde ha puesto su dispositivo o si se lo han robado o lo ha perdido, con la función Antirrobo puede localizarlo y llevar a cabo acciones remotas. Toque **LOCALIZAR** para conocer la ubicación de su dispositivo. Se mostrará la última posición conocida, junto con la fecha y la hora.
- **Vulnerabilidad.** Para comprobar las vulnerabilidades de un dispositivo, como por ejemplo actualizaciones de Windows sin hacer, aplicaciones obsoletas o contraseñas débiles, toque 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. Toque **Más detalles** para acceder a un informe pormenorizado acerca de los problemas encontrados.

2.3.8. 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.

2.4. Mantener 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 dispositivo y cada **hora** a partir de ese momento. Si se detecta una actualización, esta es automáticamente descargada e instalada en su dispositivo.

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 dispositivo se conecta a internet a través de un servidor proxy, puede configurar las opciones del proxy según se describe en .
- Si está conectado a internet a través de una conexión por módem analógico, es recomendable actualizar Bitdefender manualmente. Para más información, diríjase a .

2.4.1. 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.

2.4.2. 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**
> Puede que sea necesario reiniciar el dispositivo cuando haya finalizado 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. Acceso Centro de Bitdefender.
2. Selecciona el **Mis dispositivos** panel.
3. Haga clic en la tarjeta del dispositivo deseado y luego en el ⋮ icono en la esquina superior derecha de la pantalla.
4. Seleccionar **Actualizar**.

2.4.3. Activar o desactivar la actualización automática

Para activar o desactivar la actualización automática:

1. Hacer clic **Ajustes** en el menú de navegación de la Interfaz de Bitdefender.
2. Seleccione la pestaña **Actualización**.
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.

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

2.4.4. 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. Hacer clic **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 dispositivo. 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**.

2.4.5. 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 2020 instalado.

3. GESTIÓN DE SU SEGURIDAD

3.1. Protección Antivirus

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

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

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

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

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

Bitdefender analiza automáticamente cualquier dispositivo extraíble que se conecte a su dispositivo para así asegurarse de que se puede acceder al mismo de forma segura. Para más información, diríjase a Análisis automático de los medios extraíbles (página 59).

Los usuarios avanzados pueden configurar excepciones de análisis si no desean que se analicen ciertos archivos o tipos de archivo. Para más información, diríjase a Configurar excepciones de análisis (página 61).

Cuando detecte una amenaza, Bitdefender intentará eliminar automáticamente el código malicioso del archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección. Los archivos que no pueden ser desinfectados se mueven a la cuarentena con el fin de contener la infección. Para más información, diríjase a Administración de los archivos en cuarentena (página 63).

Si su dispositivo se ha visto infectado con amenazas, consulte Eliminación de amenazas de su sistema (página 103). Para ayudarle a limpiar su dispositivo de amenazas que no pueden eliminarse desde el propio sistema operativo Windows, Bitdefender le ofrece Entorno de rescate. Este es un entorno de confianza, especialmente diseñado para la eliminación de amenazas, lo que le permite arrancar el dispositivo independientemente de Windows. Cuando el dispositivo se ejecuta en Entorno de rescate, las amenazas de Windows están inactivas, por lo que es fácil eliminarlas.

3.1.1. 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.

Activar o desactivar la protección en tiempo real

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

1. Haga clic en **Protección** en el menú de navegación de la **interfaz de Bitdefender**.
2. En el panel **ANTIVIRUS**, haga clic en **Abrir**.
3. En la ventana **Avanzado**, active o desactive **Bitdefender Residente**.
4. Si desea desactivar la protección en tiempo real, aparecerá una ventana de advertencia. Debe confirmar su elección seleccionando en el menú cuanto tiempo desea que la protección en tiempo real esté desactivada. Puede desactivar la protección en tiempo real durante cinco, quince o treinta minutos, durante una hora, de forma permanente o hasta que se reinicie el sistema. La protección en tiempo real se activará automáticamente cuando finalice el tiempo seleccionado.

Advertencia

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

Configuración de los ajustes avanzados de la protección en tiempo real

Los usuarios avanzados podrían querer aprovechar las ventajas de las opciones de análisis que ofrece Bitdefender. Puede configurar los ajustes

de la protección en tiempo real en detalle creando un nivel de protección personalizado.

Para configurar los ajustes avanzados de la protección en tiempo real:

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

Información sobre las opciones de análisis

Puede que esta información le sea útil:

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

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

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

- **Analizar los sectores de arranque.** Puede configurar Bitdefender para que analice los sectores de arranque de su disco duro. Este sector del disco duro contiene el código informático necesario para iniciar el proceso de arranque. Cuando una amenaza infecta el sector de arranque, la unidad podría volverse inaccesible y ser incapaz de iniciar su sistema y acceder a sus datos.

- **Analizar solo los archivos nuevos o modificados.** Al analizar únicamente los archivos nuevos o modificados, puede mejorar en gran medida la capacidad de respuesta general del sistema comprometiendo mínimamente la seguridad.

- **Analizar en busca de keyloggers.** Seleccione esta opción para analizar su sistema en busca de aplicaciones keylogger. Los keyloggers registran lo que escribe en el teclado y envían informes por Internet a alguien con malas intenciones (hacker). El pirata informático puede hallar información confidencial en los datos robados, como números de cuentas bancarias y contraseñas, y utilizarla en su propio beneficio.

- **Análisis de arranque.** Seleccione la opción de **Análisis de arranque** para analizar su sistema al iniciarse, tan pronto como se hayan cargado todos los servicios críticos. La finalidad de esta característica es mejorar la detección de amenazas en el inicio del sistema, así como el tiempo de arranque del mismo.

Medidas adoptadas sobre las amenazas detectadas

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

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

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

Tomar las medidas adecuadas

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

- **Archivos infectados.** Los archivos detectados como infectados coinciden con la información sobre amenazas encontrada en la base de datos de Bitdefender. Bitdefender intentará automáticamente eliminar el código malicioso del archivo infectado y reconstruir el archivo original. Esta operación se conoce como desinfección.

  Los archivos que no pueden ser desinfectados se mueven a la cuarentena con el fin de contener la infección. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Para más información, diríjase a {1}{2}.

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

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

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

Pasar a la cuarentena

Traslada los archivos detectados a la cuarentena. Los archivos en cuarentena no pueden ejecutarse ni abrirse; en consecuencia, desaparece el riesgo de resultar infectado. Para más información, diríjase a Administración de los archivos en cuarentena (página 63).

Denegar el acceso

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

Restaurar la configuración predeterminada

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

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

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

3.1.2. Análisis solicitado

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

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

El análisis bajo demanda está basado en tareas de análisis. Las tareas de análisis especifican las opciones de análisis y los objetos a analizar. Puede analizar el dispositivo siempre que quiera ejecutando las tareas predeterminadas o sus propias tareas de análisis (tareas definidas por el usuario). Si desea analizar ubicaciones específicas en el dispositivo o configurar las opciones de análisis, configure y ejecute un análisis personalizado.

Analizar un archivo o una carpeta en busca de amenazas

Debe analizar los archivos y carpetas cuando sospeche que puedan estar infectados. Haga clic con el botón derecho en el archivo o carpeta que desee analizar, escoja **Bitdefender** y seleccione **Analizar con Bitdefender**. Aparecerá el **Asistente de análisis antivirus** que le guiará durante este proceso. Al final del análisis, se le pedirá que elija las acciones que desea llevar a cabo sobre los archivos detectados, si se encontrase alguno.

Ejecución de un análisis Quick Scan

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

Para ejecutar un análisis Quick Scan:

1. Haga clic en Protección en el menú de navegación de la interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. En la ventana de **Análisis**, haga clic en el botón **Ejecutar análisis** junto a **Quick Scan**.
4. Siga el **Asistente de análisis antivirus** para completar el análisis. Bitdefender aplicará automáticamente las acciones recomendadas sobre los archivos detectados. Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas.

Ejecución de un análisis del sistema

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

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

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

- Asegúrese de que Bitdefender está actualizado con su base de datos de información de amenazas. Analizar su dispositivo con una base de datos de información de amenazas obsoleta puede impedir que Bitdefender detecte nuevas amenazas encontradas desde la última actualización. Para más información, diríjase a Mantener Bitdefender al día (página 40).
- Cierre todos los programas abiertos.

Si desea analizar ubicaciones específicas en el dispositivo o configurar las opciones de análisis, configure y ejecute un análisis personalizado. Para más información, diríjase a Configuración de un análisis personalizado (página 52).

Para ejecutar un Análisis del sistema:

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

Configuración de un análisis personalizado

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

Para configurar detalladamente un nuevo análisis personalizado:

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

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

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

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

Información sobre las opciones de escaneo

Usted puede encontrar esta información útil:

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

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

- **Análisis de archivos comprimidos.** Los archivos comprimidos que contienen archivos infectados no representan una amenaza inmediata para la seguridad del sistema. Las amenazas pueden afectar a su sistema solo si el archivo infectado es extraído del archivo comprimido y ejecutado sin tener la protección en tiempo real activada. No obstante, se recomienda usar esta opción con el fin de detectar y eliminar cualquier amenaza potencial, incluso aunque no se trate de una amenaza inmediata.

  Arrastre el control deslizante por la escala para excluir del análisis los archivos que superen determinado tamaño indicado en MB (Megabytes).

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

- **Escanee solo archivos nuevos y modificados.** Al escanear solo archivos nuevos y modificados, puede mejorar en gran medida la capacidad de respuesta general del sistema con una compensación mínima en seguridad.
- **Escanear sectores de arranque.** Puede configurar Bitdefender para escanear los sectores de arranque de su disco duro. Este sector del disco duro contiene el código informático necesario para iniciar el proceso de arranque. Cuando una amenaza infecta el sector de arranque, la unidad puede volverse inaccesible y es posible que no pueda iniciar su sistema y acceder a sus datos.
- **Analizar la memoria.** Seleccione esta opción para analizar programas que se ejecuten en la memoria de su sistema.
- **Analizar el Registro.** Seleccione esta opción para analizar las claves del Registro. El Registro de Windows es una base de datos que almacena los ajustes de configuración y opciones para los componentes

del sistema operativo Windows, además de para las aplicaciones instaladas.

- **Analizar las cookies.** Seleccione esta opción para analizar las cookies almacenadas por los navegadores en su dispositivo.
- **Escanear registradores de teclas.** Seleccione esta opción para escanear su sistema en busca de aplicaciones de registro de teclas. Los keyloggers registran lo que escribe en su teclado y envían informes a través de Internet a una persona malintencionada (hacker). El pirata informático puede encontrar información confidencial de los datos robados, como números de cuentas bancarias y contraseñas, y utilizarla para obtener beneficios personales.

Asistente del análisis Antivirus

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

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

Paso 1 - Ejecutar análisis

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

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

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

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

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

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

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

Paso 2 - Elegir acciones

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

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

Los objetos infectados se muestran en grupos, según las amenazas con las que estén infectados. Haga clic en el enlace correspondiente a una amenaza para obtener más información sobre los objetos infectados.

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

Tomar las medidas adecuadas

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

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

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

Los archivos que no se pueden desinfectar se mueven a la cuarentena para contener la infección. Los archivos en cuarentena no se pueden ejecutar ni abrir; por lo tanto, el riesgo de infectarse desaparece. Para obtener más información, consulte Administración de los archivos en cuarentena (página 63).

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

- **Archivos sospechosos.** El análisis heurístico detecta los archivos como sospechosos. Los archivos sospechosos no se pueden desinfectar porque no hay una rutina de desinfección disponible. Serán trasladados a cuarentena para prevenir una posible infección.

  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 que contienen archivos infectados.**
  - Los archivos que contienen solo archivos infectados se eliminan automáticamente.
  - Si un archivo contiene archivos infectados y limpios, Bitdefender intentará eliminar los archivos infectados siempre que pueda reconstruir el archivo con los archivos limpios. Si la reconstrucción del archivo no es posible, se le informará que no se puede tomar ninguna medida para evitar la pérdida de archivos limpios.

Eliminar

Elimina los archivos detectados del disco.

Si se almacenan archivos infectados junto con archivos limpios en un mismo paquete, Bitdefender intentará limpiar los archivos infectados y reconstruir el paquete con los limpios. Si es imposible la reconstrucción

del archivo empaquetado, se le informará de que no puede aplicarse ninguna acción para evitar perder archivos limpios.

No realizar ninguna acción

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

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

Paso 3 – Resumen

Una vez BitDefender ha finalizado la reparación de los problemas, aparecerán los resultados del análisis en una nueva ventana. Si desea información completa sobre el proceso de análisis, haga clic en **MOSTRAR REGISTRO** para ver el registro de análisis.

> **Importante**
> En la mayoría de casos, BitDefender desinfecta los archivos infectados detectados o aísla estos archivos en la Cuarentena. Sin embargo, hay incidencias que no pueden resolverse automáticamente. En caso necesario, reinicie su equipo para completar el proceso de desinfección. Para obtener más información e instrucciones sobre cómo eliminar manualmente una amenaza, consulte Eliminación de amenazas de su sistema (página 103).

3.1.3. Comprobación de los resultados del análisis

Cada vez que se realiza un análisis, se crea un registro del mismo y Bitdefender graba los problemas detectados en la ventana del antivirus. El informe de análisis detalla información sobre el proceso de análisis, como las opciones del análisis, el objetivo del análisis, las amenazas detectadas y las acciones realizadas.

Puede abrir el registro de análisis directamente desde el asistente de análisis, una vez finalizado este, haciendo clic en **MOSTRAR REGISTRO**.

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

1. Hacer clic **Notificaciones** en el menú de navegación de la Interfaz de Bitdefender.
2. En la pestaña **Todos**, seleccione la notificación correspondiente al último análisis.

Aquí es donde puede encontrar todos los eventos de análisis de amenazas, incluyendo las detectadas por los análisis en tiempo real, análisis iniciados por el usuario y cambios de estado para análisis automáticos.

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

3.1.4. Análisis automático de los medios extraíbles

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

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

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

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

¿Cómo funciona?

Cuando se detecta un dispositivo de almacenamiento extraíble, Bitdefender inicia el análisis en busca de amenazas (siempre y cuando se haya habilitado el análisis automático para este tipo). Mediante una ventana emergente se le notificará que se ha detectado un nuevo dispositivo y se está analizando.

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

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

En la mayoría de los casos, Bitdefender elimina automáticamente las amenazas detectadas o mantiene aislados en cuarentena los archivos infectados. Si quedan amenazas sin resolver tras el análisis, se le pedirá que elija las acciones a adoptar relativas a las mismas.

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

Esta información le puede ser útil:

- Tenga cuidado al usar un CD/DVD infectado con una amenaza, porque esta no puede eliminarse del disco (el soporte es de solo lectura). Asegúrese de que la protección en tiempo real está activada para evitar que las amenazas se propaguen por su sistema. Es una buena práctica copiar los datos importantes desde el disco a su sistema y luego deshacerse de los discos.
- En algunos casos, Bitdefender puede no ser capaz de eliminar amenazas de determinados archivos debido a restricciones legales o técnicas. Un ejemplo son los archivos comprimidos con una tecnología propia (esto es porque el archivo no se puede recrear correctamente). Para averiguar cómo enfrentarse a las amenazas, consulte Eliminación de amenazas de su sistema (página 103).

Administrar el análisis de medios extraíbles

Para gestionar el análisis automático de medios extraíbles:

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

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

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

3.1.5. 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**.

Exceptuar del análisis los archivos o carpetas

Para exceptuar determinados archivos y carpetas del análisis:

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

- Antivirus
- Prevención de amenazas online
- Advanced Threat Defense

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

Exceptuar del análisis las extensiones de archivo

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

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

Para exceptuar extensiones de archivo del análisis:

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

Administrar excepciones de análisis

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

Para administrar las excepciones del análisis:

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

3.1.6. 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.

De forma predeterminada, los archivos en cuarentena se envían automáticamente a Bitdefender Labs para que los analicen los investigadores de amenazas de Bitdefender. Si se confirma la presencia de una amenaza, se publica una actualización de la información para permitir eliminar la amenaza.

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

Para comprobar y administrar los archivos en cuarentena:

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

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

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

3.2. Defensa contra amenazas avanzadas

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

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

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

3.2.1. Activar o desactivar Defensa Contra Amenazas Avanzadas

Para activar o desactivar Defensa Contra Amenazas Avanzadas:

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

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

3.2.2. Comprobación de los ataques maliciosos detectados

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

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

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

3.2.4. 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 dispositivo permanezca a salvo de esos ataques, que normalmente se propagan muy rápidamente, Bitdefender utiliza las tecnologías antiexploit más recientes.

3.2.5. Activar o desactivar la detección de exploits

Para activar o desactivar la detección de exploits:

- Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
- En el **DEFENSA AVANZADA CONTRA AMENAZAS** panel, haga clic **Abierto**.
- Acceda a la ventana **Ajustes** y haga clic en el conmutador junto a **Detección de exploits** para activar o desactivar la característica.

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

3.3. Prevención de amenazas en línea

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

Bitdefender proporciona prevención de amenazas online en tiempo real para:

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

Para configurar los ajustes de la Prevención de amenazas online:

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

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

- La prevención de ataques web bloquea las amenazas procedentes de Internet, incluyendo las descargas ocultas.
- Asesor de búsqueda, un componente que califica los resultados de las consultas en su motor de búsqueda y los enlaces publicados en sitios Web de redes sociales añadiendo un icono junto a cada resultado:

  No debería visitar esta página web.

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

  Esta es una página segura.

  El Asesor de búsqueda califica los resultados de los siguientes motores de búsqueda:

  - Google

- Yahoo!
- Bing
- Baidu

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

- Facebook
- Twitter

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

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

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

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

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **PREVENCIÓN DE AMENAZAS EN LÍNEA** panel, haga clic **Ajustes**.
3. Haga clic en **Administrar excepciones**.
4. Hacer clic **+Agregar una excepción**.

5. Escriba en el campo correspondiente el nombre del sitio web, el nombre del dominio o la dirección IP que desea añadir a las excepciones.
6. Haga clic en el conmutador junto a **Prevención de amenazas online**.
7. Para eliminar una entrada de la lista, haga clic en el botón botón al lado.
   Hacer clic **Ahorrar** para guardar los cambios y cerrar la ventana.

3.3.1. 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 qué hacer a continuación. Tiene a su disposición las siguientes opciones:

- Abandone el sitio web haciendo clic en **LLÉVAME A UN SITIO SEGURO**.
- Dirigirse al sitio Web, a pesar de la advertencia, haciendo clic en **Estoy informado acerca de los riesgos, visitar la página de todos modos**.
- Si sabe a ciencia cierta que el sitio web detectado es seguro, haga clic en **ENVIAR** para añadirlo a la lista blanca. Le recomendamos que solo añada sitios web en los que confíe plenamente.

4. CÓMO

4.1. Instalación

4.1.1. ¿Cómo instalo Bitdefender en un segundo dispositivo?

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

Para instalar Bitdefender en un segundo dispositivo:

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

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

4.1.2. ¿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.

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

- En **ventanas 7**:
  1. Hacer clic **Comenzar** E ir a **Todos los programas**.
  2. Busque *Bitdefender Antivirus Free* y seleccione **Desinstalar**.
  3. Haga clic en **REINSTALAR** en la ventana que aparece.
  4. Necesita reiniciar el dispositivo para completar el proceso.

- En **ventanas 8** y **Windows 8.1**:
  1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
  2. Haga clic en **Desinstalar un programa** o **Programas y características**.
  3. Encontrar **Bitdefender Antivirus Free** y seleccione **Desinstalar**.
  4. Hacer clic **REINSTALAR** en la ventana que aparece.
  5. Debe reiniciar el dispositivo para completar el proceso.
- En **ventanas 10** y **ventanas 11**:
  1. Haga clic en **Inicio** y, a continuación, haga clic en **Ajustes**.
  2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones y características**.
  3. Encontrar **Bitdefender Antivirus Free** y seleccione **Desinstalar**.
  4. Haga clic en **Desinstalar** para confirmar su elección.
  5. Haga clic en **REINSTALAR**.
  6. Debe reiniciar el dispositivo para completar el proceso.

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

4.1.3. ¿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 dispositivo desde la plataforma de Bitdefender Central.

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

Para instalar Bitdefender desde Bitdefender Central:

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

4.1.4. ¿Cómo puedo actualizar a la última versión de Bitdefender?

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

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

1. Haga clic en **REINICIAR AHORA** en la notificación que reciba con la información de actualización. Si la pasa por alto, acceda a la

ventana **Notificaciones**, seleccione la actualización más reciente y, a continuación, haga clic en el botón **REINICIAR AHORA**. Espere a que se reinicie el dispositivo.

Aparece la ventana **Novedades** con información sobre las características nuevas y mejoradas.

2. Haga clic en el enlace **Más información** para leer una página con más detalles y artículos útiles.
3. Cierre la ventana **Novedades** para acceder a la interfaz de la nueva versión instalada.

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

4.2. Centro de Bitdefender

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

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

Para poder iniciar sesión con otra cuenta de Bitdefender:

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

> **Nota**
> El producto Bitdefender de su dispositivo cambia automáticamente de acuerdo con la suscripción asociada a la nueva cuenta de Bitdefender. Si no hay ninguna suscripción disponible asociada a la nueva cuenta de Bitdefender, o si desea transferirla desde la cuenta anterior, puede ponerse en contacto con el soporte técnico de Bitdefender como se describe en la sección Solicitando Ayuda (página 110).

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

4.2.3. 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 el Interfaz de Bitdefender:
  1. Hacer clic **Mi cuenta** en el menú de navegación de la Interfaz de Bitdefender.
  2. Haga clic en **Cambiar cuenta** en la esquina superior derecha de la pantalla.
     Aparecerá una nueva ventana.
  3. Escriba su dirección de correo electrónico y haga clic en **SIGUIENTE**.
     Aparece una nueva ventana.
  4. Hacer clic **¿Has olvidado tu contraseña?**.

5. Haga clic en **SIGUIENTE**.
6. Verifique su cuenta de correo electrónico, escriba el código de seguridad que ha recibido y luego haga clic en **PRÓXIMO**.
   Como alternativa, puede hacer clic en **Cambiar la contraseña** en el correo que te enviamos.
7. Escriba la nueva contraseña que desea establecer y luego escríbala una vez más. Hacer clic **AHORRAR**.

- Desde su navegador web:
  1. Ir a: https://central.bitdefender.com.
  2. Haga clic en **INICIAR SESIÓN**.
  3. Escriba su dirección de correo electrónico y luego haga clic en **PRÓXIMO**.
  4. Hacer clic **¿Has olvidado tu contraseña?**.
  5. Hacer clic **PRÓXIMO**.
  6. Revise su cuenta de correo electrónico y siga las instrucciones que se le proporcionan para establecer una nueva contraseña para su cuenta Bitdefender.

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

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

4.3. Analizando con BitDefender

4.3.1. ¿Cómo analizo un archivo o una carpeta?

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

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

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

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

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

4.3.2. ¿Cómo analizo mi sistema

Para llevar a cabo un análisis completo del sistema:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. Haga clic en el botón **Ejecutar análisis** junto a **Análisis del sistema**.
4. Siga el Asistente de análisis del sistema para completar el análisis. Bitdefender aplicará automáticamente las acciones recomendadas sobre los archivos detectados.
   Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas. Para más información, diríjase a .

4.3.3. ¿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 dispositivo.

Para programar un análisis:

1. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
2. En el **ANTIVIRUS** panel, haga clic **Abierto**.
3. Haga clic en ··· junto al tipo de análisis que desea programar: Análisis del sistema o Quick Scan, en la parte inferior de la interfaz y, a continuación, seleccione **Editar**.
   Como alternativa, puede crear un tipo de análisis que se adapte a sus necesidades haciendo clic en **+Crear análisis** junto a **Administrar análisis**.
4. Personalice el análisis según sus necesidades y, a continuación, haga clic en **Siguiente**.
5. Marque la casilla junto a **Elegir para cuándo programar esta tarea**.
   Seleccione una de las opciones correspondientes para establecer una programación:
   - Al inicio del sistema
   - A diario
   - Semanalmente
   - Mensual

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

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

4.3.4. ¿Cómo creo una tarea de análisis personalizada?

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

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

1. En el **ANTIVIRUS** panel, haga clic **Abierto**.
2. Haga clic en **+Crear análisis** junto a **Administrar análisis**.
3. En el campo de nombre de la tarea, escriba un nombre para el análisis, seleccione las ubicaciones que le gustaría analizar y, a continuación, haga clic en **SIGUIENTE**.
4. Configure estas opciones generales:
   - **Analizar únicamente aplicaciones**. Puede configurar Bitdefender para analizar solo las aplicaciones a las que accede.
   - **Prioridad de la tarea de análisis**. Puede elegir el impacto que el proceso de análisis debería tener en el rendimiento de su sistema.
     - Automático: la prioridad del proceso de escaneo dependerá de la actividad del sistema. Para asegurarse de que el proceso de análisis no afecte a la actividad del sistema, Bitdefender decidirá si el proceso de análisis debe ejecutarse con prioridad alta o baja.
     - Alta: la prioridad del proceso de escaneo será alta. Al elegir esta opción, permitirá que otros programas se ejecuten más lentamente y disminuirá el tiempo necesario para que finalice el proceso de escaneo.
     - Baja: la prioridad del proceso de escaneo será baja. Al elegir esta opción, permitirá que otros programas se ejecuten más rápido y aumentará el tiempo necesario para que finalice el proceso de escaneo.
   - **Acciones posteriores al análisis**. Elija la acción que debe llevar a cabo Bitdefender en caso de que no se encuentren amenazas:
     - Mostrar ventana Resumen
     - Dispositivo de apagado
     - Cerrar ventana de escaneo
5. Si desea configurar detalladamente las opciones de análisis, haga clic en **Mostrar opciones avanzadas**.

Hacer clic **Próximo**.

6. Si lo desea, puede habilitar la opción **Programar tarea de análisis** y, a continuación, elegir cuándo debe iniciarse el análisis personalizado que ha creado.
   - Al inicio del sistema
   - A diario
   - Mensual
   - Semanalmente

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

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

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

4.3.6. ¿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. Desactivar la protección antivirus en tiempo real de Bitdefender:
   a. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
   b. En el **ANTIVIRUS** panel, haga clic **Abierto**.
   c. En la ventana **Avanzado**, desactive **Bitdefender Residente**.
   Aparecerá una ventana de advertencia. Debe confirmar su elección seleccionando en el menú cuanto tiempo desea que la protección en tiempo real esté desactivada. Puede desactivar la protección en

tiempo real durante cinco, quince o treinta minutos, durante una hora, de forma permanente o hasta que se reinicie el sistema.

2. Muestre los objetos ocultos en Windows. Para averiguar cómo hacerlo, consulte ¿Cómo puedo mostrar los objetos ocultos en Windows? (página 87).
3. Restaurar el archivo desde el área de Cuarentena:
   a. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
   b. En el **ANTIVIRUS** panel, haga clic **Abierto**.
   c. Acceda a la ventana **Ajustes** y haga clic en **Administrar cuarentena**.
   d. Seleccione el archivo y, a continuación, haga clic en **Restaurar**.
4. Añada el archivo a la lista de excepciones. Para averiguar cómo hacerlo, consulte ¿Cómo puedo evitar que se analice una carpeta? (página 79).
5. Active la protección antivirus en tiempo real de Bitdefender.
6. Póngase en contacto con nuestros agentes de soporte técnico para que podamos eliminar la detección de la actualización de información sobre amenazas. Para averiguar cómo hacerlo, consulte Solicitando Ayuda (página 110).

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

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

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

4.4. Información de Utilidad

4.4.1. ¿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 Solicitando Ayuda (página 110).

4.4.2. ¿Cómo desinstalo Bitdefender?

Si desea eliminar su Bitdefender Antivirus Free :

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

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

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

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

4.4.3. ¿Cómo apago el dispositivo automáticamente después de que finalice el análisis?

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

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

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

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

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

Para apagar el dispositivo al finalizar un análisis personalizado:

1. Haga clic en ⋯ junto al análisis personalizado que ha creado.
2. Haga clic en **Siguiente** y, a continuación, haga clic otra vez en **Siguiente**.

3. Marque la casilla junto a **Elegir para cuándo programar esta tarea** y, a continuación, elija cuándo debe comenzar la tarea.
4. Hacer clic **Ahorrar**.

Si no se encuentran amenazas, su dispositivo se apagará.

Si quedan amenazas sin resolver, se le pedirá que elija las acciones a adoptar relativas a las mismas. Para más información, diríjase a Asistente del análisis Antivirus (página 55).

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

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

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

Para administrar las opciones del proxy:

1. Hacer clic **Ajustes** en el menú de navegación de la Interfaz de Bitdefender.
2. Selecciona el **Avanzado** pestaña.
3. Active el **Servidor proxy**.
4. Haga clic en **Cambio de proxy**.
5. Hay dos opciones para establecer la configuración del proxy:
   - **Importar configuración proxy desde el navegador predeterminado** - la configuración del proxy del usuario actual, extraída del navegador predeterminado. Si el servidor proxy necesita nombre de usuario y contraseña, deberá indicarlos en los campos correspondientes.

> **Nota**
> Bitdefender puede importar la configuración proxy desde los navegadores más populares, incluyendo las últimas versiones de Microsoft Edge, Internet Explorer, Mozilla Firefox y Google Chrome.

- **Configuración personalizada del proxy** - la configuración del proxy que puede modificar.
  Deben indicarse las siguientes opciones:
  - **Dirección**: Introduzca la dirección IP del servidor proxy.
  - **Puerto**: Introduzca el puerto que Bitdefender utiliza para conectar con el servidor proxy.
  - **Nombre de usuario**: Introduzca un nombre de usuario que el proxy reconozca.
  - **Contraseña**: Escriba una contraseña válida para el usuario especificado anteriormente.

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

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

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

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

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

- En **Windows 8**:
  1. Desde la pantalla de inicio de Windows, localice **Equipo** (por ejemplo, puede empezar escribiendo "Equipo" directamente en la pantalla Inicio) luego haga clic con el botón derecho sobre su icono.

En **Windows 8.1**, busque **Este PC**.

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

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

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

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

Estos pasos son útiles cuando se enfrenta a una amenaza y necesita encontrar y eliminar los archivos infectados, que podrían estar ocultos.

Siga estos pasos para ver los elementos ocultos de Windows:

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

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

1. Escriba "Mostrar todos los archivos y carpetas ocultos" en el cuadro de búsqueda de la barra de tareas y luego haga clic en su icono.
2. Seleccione {1}Mostrar archivos, carpetas y unidades ocultos{2}.
3. Claro **Ocultar las extensiones para tipos de archivo conocidos**.

4. Claro **Ocultar archivos protegidos del sistema operativo**.
5. Hacer clic **Aplicar**, luego haga clic **DE ACUERDO**.

4.4.7. ¿Cómo desinstalo otras soluciones de seguridad?

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

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

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

- En **ventanas 7**:
  1. Hacer clic **Comenzar**, ir a **Panel de control** y haga doble clic **Programas y características**.
  2. Espere un momento a que el software instalado se muestre.
  3. Encuentre el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  4. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.

- En **ventanas 8** y **Windows 8.1**:
  1. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control" directamente en la pantalla de inicio) y luego hacer clic en su icono.
  2. Hacer clic **Desinstalar un programa** o **Programas y características**.
  3. Espere unos momentos hasta que se muestre la lista de software instalado.
  4. Busque el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  5. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.

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

  1. Hacer clic **Comenzar**y luego haga clic en Configuración.
  2. Haga clic en el **Sistema** en el área de Configuración, luego seleccione **aplicaciones**.
  3. Busque el nombre del programa que desea eliminar y seleccione **Desinstalar**.
  4. Hacer clic **Desinstalar** de nuevo para confirmar su elección.
  5. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.

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

4.4.8. ¿Cómo puedo reiniciar en Modo Seguro?

El Modo Seguro es un modo de diagnóstico operativo, utilizado principalmente para resolver problemas que afectan a la operación normal de Windows. Dichos problemas van desde controladores en conflicto hasta amenazas que impiden que Windows se inicie normalmente. En Modo Seguro solo una cuantas aplicaciones trabajan y Windows carga solo los controladores básicos y un mínimo de componentes del sistema operativo. Por esta razón la mayoría de las amenazas están inactivas cuando se usa Windows en modo seguro y se pueden eliminar fácilmente.

Para iniciar Windows en Modo Seguro:

- En **ventanas 7**:

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

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

- En **Windows 8**, **Windows 8.1**, **Windows 10** y **Windows 11**:
  1. Acceda a la **Configuración del sistema** en Windows pulsando al mismo tiempo las teclas **Windows y R**.
  2. Escriba **msconfig** en el campo **Abrir** del cuadro de diálogo y, a continuación, haga clic en **Aceptar**.
  3. Seleccione la pestaña **Arranque**.
  4. En la sección de **Opciones de arranque**, marque la casilla de verificación **Arranque a prueba de errores**.
  5. Haga clic en **Red** y, a continuación, haga clic en **Aceptar**.
  6. Haga clic en **Aceptar** en la ventana de **Configuración del sistema** que le informa de que el sistema debe reiniciarse para realizar los cambios que acaba de establecer.
     Su sistema se reiniciará en modo seguro con funciones de red.

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

5. RESOLUCIÓN DE PROBLEMAS

5.1. Resolución de incidencias comunes

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

- Mi sistema parece que se ejecuta lento (página 91)
- El análisis no se inicia (página 93)
- Ya no puedo usar una app (página 95)
- Qué hacer cuando Bitdefender bloquea un sitio web, un dominio, una dirección IP o una aplicación online que son seguros (página 96)
- Cómo actualizo Bitdefender en una conexión de internet lenta (página 97)
- Los servicios de Bitdefender no responden (página 98)
- El Filtro antispam no funciona correctamente
- Error al eliminar Bitdefender (página 99)
- Mi sistema no se inicia tras la instalación de Bitdefender (página 100)

Si no puede encontrar su problema aquí, o si la solución presentada no lo resuelve, puede contactar con el soporte técnico de BitDefender como se representa en el capítulo Solicitando Ayuda (página 110).

5.1.1. 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 el único programa de seguridad instalado en el sistema.**
  Aunque Bitdefender busca y elimina los programas de seguridad encontrados durante la instalación, se recomienda eliminar cualquier

otra solución de seguridad que pueda usar antes de instalar Bitdefender. Para más información, diríjase a ¿Cómo desinstalo otras soluciones de seguridad? (página 88).

- **No se cumplen los requisitos del sistema para ejecutar Bitdefender.**
  Si su dispositivo no cumple los requisitos del sistema, se ralentiza, especialmente cuando se ejecutan varias aplicaciones al mismo tiempo. Para más información, diríjase a Requisitos del sistema (página 4).

- **Ha instalado apps que no utiliza.**
  Cualquier dispositivo tiene programas o aplicaciones que no utiliza. Y muchos programas no deseados se ejecutan en segundo plano ocupando espacio en disco y memoria. Si no utiliza un programa, desinstálelo. Esto también vale para otro software preinstalado o aplicación de evaluación que olvidó desinstalar.

  > **Importante**
  > Si sospecha que un programa o una aplicación forma parte esencial de su sistema operativo, no lo elimine y contacte con el departamento de Atención al cliente de Bitdefender para recibir asistencia.

- **Su sistema puede estar infectado.**
  La velocidad de su sistema y su comportamiento general también pueden verse afectados por las amenazas. Spyware, malware, troyanos y adware pasan todos factura al rendimiento de su dispositivo. No olvide analizar su sistema regularmente; al menos una vez a la semana. Se recomienda utilizar el análisis del sistema de Bitdefender porque analiza todo los tipos de amenazas que ponen en peligro la seguridad de su sistema.
  Para iniciar el análisis del sistema:

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

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

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

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

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

  1. Eliminar las otras soluciones de seguridad. Para más información, diríjase a ¿Cómo desinstalo otras soluciones de seguridad? (página 88).
  2. Reinstale Bitdefender:
     - En **ventanas 7**:
       a. Hacer clic **Comenzar**, ir a **Panel de control** y haga doble clic **Programas y características**.
       b. Encontrar **Bitdefender Antivirus Free** y seleccione **Desinstalar**.
       c. Hacer clic **REINSTALAR** en la ventana que aparece.
       d. Espere a que se complete el proceso de reinstalación y luego reinicie su sistema.
     - En **ventanas 8** y **Windows 8.1**:
       a. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control" directamente en la pantalla de inicio) y luego hacer clic en su icono.
       b. Hacer clic **Desinstalar** un programa o **Programas y características**.
       c. Encontrar **Bitdefender Antivirus Free** y seleccione **Desinstalar**.
       d. Hacer clic **REINSTALAR** en la ventana que aparece.

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

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

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

Si esta información no le ayuda, puede contactar con el Soporte de BitDefender como se describe en la sección Solicitando Ayuda (página 110).

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

Si esta información no fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 110).

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

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

Si esta información no fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 110).

5.1.5. Cómo actualizo Bitdefender en una conexión de internet lenta

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

Para mantener su sistema actualizado con la última base de datos de información de amenazas de Bitdefender:

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

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

5.1.6. Los servicios de Bitdefender no responden

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

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

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

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

Para solucionar este problema, pruebe estas soluciones:

1. Espere unos momentos y mire si algo cambia. El error puede ser temporal.
2. Reinicie el dispositivo y espere unos momentos a que Bitdefender se inicie. Abra BitDefender para ver si el error continua. Reiniciando el dispositivo normalmente soluciona el problema.
3. Compruebe si tiene alguna otra solución de seguridad instalada porque esta puede perturbar la ejecución normal de BitDefender. Si este es el caso, le recomendamos que elimine todas las otras soluciones de seguridad y reinstale BitDefender.
   Para más información, diríjase a ¿Cómo desinstalo otras soluciones de seguridad? (página 88).

Si el error persiste y contacte con nuestros representantes de soporte para conseguir ayuda según se describe en la sección Solicitando Ayuda (página 110).

5.1.7. Error al eliminar Bitdefender

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

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

Para eliminar Bitdefender de su sistema por completo:

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

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

- En **ventanas 10** y **ventanas 11**:
  1. Hacer clic **Comenzar**y luego haga clic en Configuración.
  2. Haga clic en el **Sistema** en el área de Configuración, luego seleccione **aplicaciones instaladas**.
  3. Encontrar **Bitdefender Antivirus Free** y seleccione **Desinstalar**.

4. Hacer clic **Desinstalar** de nuevo para confirmar su elección.
5. Hacer clic **ELIMINAR** en la ventana que aparece.
6. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.

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

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

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

Así es como puede abordar cada situación:

- **Tenía Bitdefender antes y no lo eliminó correctamente.**
  Para resolver esto:
  1. Reinicie su sistema y entre en Modo seguro. Para averiguar cómo hacerlo, consulte ¿Cómo puedo reiniciar en Modo Seguro? (página 89).
  2. Elimine Bitdefender de su sistema:
     - En **ventanas 7**:
       a. Hacer clic **Comenzar**, ir a **Panel de control** y haga doble clic **Programas y características**.
       b. Encontrar **Bitdefender Antivirus Free** y seleccione **Desinstalar**.
       c. Hacer clic **ELIMINAR** en la ventana que aparece.
       d. Espere a que se complete el proceso de desinstalación y luego reinicie su sistema.
       e. Reinicie su sistema en modo normal.
     - En **ventanas 8** y **Windows 8.1**:
       a. En la pantalla de inicio de Windows, busque **Panel de control** (por ejemplo, puede comenzar a escribir "Panel de control"

directamente en la pantalla de inicio) y luego hacer clic en su icono.

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

c. Encontrar **Bitdefender Antivirus Free** y seleccione **Desinstalar**.

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

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

f. Reinicie su sistema en modo normal.

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

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

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

  c. Encontrar **Bitdefender Antivirus Free** y seleccione **Desinstalar**.

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

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

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

  g. Reinicie su sistema en modo normal.

3. Reinstale su producto Bitdefender.

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

  1. Reinicie su sistema y entre en modo seguro. Para saber cómo hacerlo, consulte ¿Cómo puedo reiniciar en Modo Seguro? (página 89).
  2. Elimine las otras soluciones de seguridad de su sistema:
     - En **ventanas 7**:

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

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

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

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

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

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

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

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

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

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

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

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

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

Para desinstalar correctamente el otro programa, diríjase a su sitio Web y ejecute su herramienta de desinstalación o contacte con ellos directamente para que le proporcionen las indicaciones para desinstalar.

3. Reinicie su sistema en modo normal y reinstale Bitdefender.

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

Para resolver esto:

1. Reinicie su sistema y entre en modo seguro. Para saber cómo hacerlo, consulte ¿Cómo puedo reiniciar en Modo Seguro? (página 89).
2. Utilice la opción Restaurar sistema de Windows para restaurar el dispositivo a un punto anterior antes de la instalación del producto Bitdefender.
3. Reinicie el sistema de modo normal y contacte con nuestros represetantes de soporte para conseguir ayuda según se describe en la sección Solicitando Ayuda (página 110).

5.2. Eliminación de amenazas de su sistema

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

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

- Entorno de rescate
- ¿Qué hacer cuando Bitdefender encuentra amenazas en su dispositivo? (página 104)
- ¿Cómo limpio una amenaza de un archivo? (página 105)
- ¿Cómo limpio una amenaza de un archivo de correo electrónico? (página 106)
- ¿Qué hacer si sospecho que un archivo es peligroso? (página 107)
- ¿Qué son los archivos protegidos con contraseña del registro de análisis? (página 108)
- ¿Qué son los elementos omitidos en el registro de análisis? (página 108)
- ¿Qué son los archivos sobre-comprimidos en el registro de análisis? (página 109)
- ¿Por qué ha eliminado automáticamente Bitdefender un archivo infectado? (página 109)

Si no puede encontrar su problema aquí, o si las soluciones presentadas no lo resuelven, puede comunicarse con los representantes de soporte

técnico de Bitdefender como se presenta en el capítulo Solicitando Ayuda (página 110).

5.2.1. ¿Qué hacer cuando Bitdefender encuentra amenazas en su dispositivo?

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

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

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

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

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

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

El primer método puede ser utilizado en modo normal:

1. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
   b. En el **ANTIVIRUS** panel, haga clic **Abierto**.
   c. En el **Avanzado** ventana, apagar **Escudo de Bitdefender**.
2. Mostrar objetos ocultos en Windows. Para saber cómo hacerlo, consulte ¿Cómo puedo mostrar los objetos ocultos en Windows? (página 87).

3. Busque la ubicación del archivo infectado (compruebe el log de análisis) y elimínelo.
4. Active la protección antivirus en tiempo real de Bitdefender.

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

1. Reinicie su sistema y entre en modo seguro. Para saber cómo hacerlo, consulte ¿Cómo puedo reiniciar en Modo Seguro? (página 89).
2. Mostrar objetos ocultos en Windows. Para saber cómo hacerlo, consulte ¿Cómo puedo mostrar los objetos ocultos en Windows? (página 87).
3. Busque la ubicación del archivo infectado (consulte el registro de análisis) y elimínelo.
4. Reiniciar su sistema e iniciar en modo normal.

Si esta información no fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 110).

5.2.2. ¿Cómo limpio una amenaza de un archivo?

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

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

Otros formatos de archivo están parcial o totalmente cerrados y Bitdefender solo puede detectar la presencia de amenazas en ellos, pero no realizar ninguna otra acción.

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

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

1. Identifique el archivo comprimido que incluye la amenaza realizando un Análisis del sistema.

2. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
   b. En el **ANTIVIRUS** panel, haga clic **Abierto**.
   c. En el **Avanzado** ventana, apagar **Escudo de Bitdefender**.
3. Vaya a la ubicación del archivo y descomprímalo utilizando una aplicación de descompresión de archivos, como WinZip.
4. Identifique el archivo infectado y elimínelo.
5. Elimine el archivo original con el fin de asegurar que la infección está eliminada totalmente.
6. Recomprime los archivos en nuevo archivo utilizando una aplicación de compresión, como WinZip.
7. Active la protección antivirus en tiempo real de Bitdefender y ejecute un análisis del sistema para asegurarse de que no hay ninguna otra infección en el sistema.

   Nota
   Es importante saber que una amenaza almacenada en un archivo comprimido no es un peligro inmediato para su sistema, ya que esta debe descomprimirse y ejecutarse para poder infectarlo.

Si esta información no fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 110).

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

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

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

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

1. Analice la base de datos de correo electrónico con Bitdefender.
2. Desactive la protección antivirus en tiempo real de Bitdefender:
   a. Hacer clic **Proteccion** en el menú de navegación de la Interfaz de Bitdefender.
   b. En el **ANTIVIRUS** panel, haga clic **Abierto**.
   c. En el **Avanzado** ventana, apagar **Escudo de Bitdefender**.
3. Abra el informe de análisis y utilice la información de identificación(Asunto, De, Para) de los mensajes infectados para localizarlos en el cliente de correo.
4. Elimina los mensajes infectados. Muchos de los clientes de correo puede mover los mensajes eliminados a la carpeta de recuperación, desde donde se pueden recuperar. Debería asegurarse que el mensaje también se eliminará de esta carpeta de recuperación.
5. Compactar la carpeta que almacena el mensaje infectado.
   - En Microsoft Outlook 2007: En el menú Archivo, haga clic en Administración de archivos de datos. Seleccione los archivos de carpetas personales (.pst) que desea compactar y haga clic en Configuración. Haga clic en Compactar ahora.
   - En Microsoft Outlook 2010/2013/2016: En el menú Archivo, haga clic en Info y luego en Configuración de cuenta (Añada o elimine cuentas, o cambie los ajustes de conexión existentes). Luego, haga clic en Archivo de datos, seleccione los archivos de carpetas personales (.pst) que desea compactar y haga clic en Configuración. Haga clic en Compactar ahora.
6. Active la protección antivirus en tiempo real de Bitdefender.

Si esta información no fue útil, puede ponerse en contacto con Bitdefender para obtener soporte como se describe en la sección Solicitando Ayuda (página 110).

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

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

Para asegurarse de que su sistema está protegido:

1. Ejecute un **Análisis del sistema** con Bitdefender. Para averiguar cómo hacerlo, consulte .
2. Si el resultado del análisis parece limpio, pero todavía tiene dudas y quiere asegurarse sobre la naturaleza del archivo, contacte con nuestros representantes de soporte de forma que puedan ayudarle.
   Para averiguar cómo hacerlo, consulte Solicitando Ayuda (página 110).

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

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

Por lo general, los elementos protegidos con contraseña son:

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

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

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

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

5.2.6. ¿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.

5.2.7. ¿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.

5.2.8. ¿Por qué ha eliminado automáticamente Bitdefender un archivo infectado?

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

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

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

6. OBTENIENDO AYUDA

6.1. Solicitando Ayuda

Bitdefender proporciona a sus clientes un nivel sin igual de soporte técnico rápido y preciso. Si tiene cualquier problema o alguna pregunta sobre su producto Bitdefender, dispone de varios recursos online para encontrar una solución o una respuesta. Además, puede ponerse en contacto con el equipo de Atención al Cliente de Bitdefender. Nuestros representantes de soporte técnico responderán a sus preguntas con diligencia y le proporcionarán la asistencia que necesite.

6.2. Recursos Online

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

- Centro de soporte de Bitdefender:
  https://www.bitdefender.es/consumer/support/
- La comunidad de expertos de Bitdefender:
  https://community.bitdefender.com/es
- Ciberpedia de Bitdefender:
  https://www.bitdefender.com/cyberpedia/

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

6.2.1. Centro de soporte de Bitdefender

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

El Centro de soporte de Bitdefender está abierto al público y puede consultarse gratuitamente. La amplia información que contiene es otro

medio de proporcionar a los clientes de Bitdefender los conocimientos técnicos y la información que necesitan. Todas las solicitudes válidas de información o informes de errores procedentes de los clientes acaban finalmente en el Centro de soporte de Bitdefender, como informes de resolución de errores, documentos técnicos o artículos informativos para complementar los archivos de ayuda del producto.

El Centro de soporte de Bitdefender está disponible en cualquier momento en la siguiente dirección: https://www.bitdefender.es/consumer/support/.

6.2.2. La comunidad de expertos de Bitdefender

La comunidad de expertos es un entorno en el que los usuarios, entusiastas y fanes de Bitdefender pueden participar, intercambiar ideas, apoyarse mutuamente y compartir sus conocimientos y soluciones. Además, es un lugar de creación de ideas y aporta valiosos comentarios a nuestros equipos de desarrollo. Los miembros de esta comunidad son usuarios experimentados de Bitdefender que se complacen en ayudar a otros en su tiempo libre. Con su inmensa contribución y su genuino esfuerzo de voluntariado, hemos creado una base de conocimientos en la que los usuarios pueden hallar respuestas y orientación, pero con un toque humano.

Aquí encontrará interesantes conversaciones con gente que usa Bitdefender en sus dispositivos. La comunidad establece una auténtica conexión entre sus miembros y hace oír su voz. Es un lugar donde se alienta la participación sabiendo que su opinión y aporte serán respetados y apreciados. Como valioso contribuyente, nos esforzamos por ofrecer un nivel sin igual de soporte técnico rápido y preciso y deseamos aproximarnos a nuestros usuarios. Con este propósito en mente hemos diseñado nuestra comunidad.

Puede encontrar la página web de nuestra comunidad de expertos aquí:

https://community.bitdefender.com/es

6.2.3. Ciberpedia de Bitdefender

Bitdefender Cyberpedia contiene toda la información que necesita conocer sobre las últimas amenazas digitales. Aquí es donde los expertos de Bitdefender dan a conocer consejos y trucos para protegerse contra piratas informáticos, vulneraciones de datos, robos de identidad e intentos de suplantación en las redes sociales.

En el siguiente enlace puede encontrar la página web de Bitdefender Cyberpedia:

https://www.bitdefender.com/cyberpedia/.

6.3. Información de contacto

La comunicación eficiente es la clave para un negocio exitoso. Desde 2001, BITDEFENDER ha establecido una reputación incuestionable al esforzarse constantemente por mejorar la comunicación para superar las expectativas de nuestros clientes y socios. Si tiene alguna pregunta, no dude en contactarnos directamente a través de nuestro Centro de soporte de Bitdefender (página 110).

https://www.bitdefender.es/consumer/support/

6.3.1. Distribuidores locales

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

Para encontrar un distribuidor de Bitdefender en su país:

1. Ir a https://www.bitdefender.com/partners/localizador-de-socios.html.
2. Elija su país y ciudad mediante las opciones correspondientes.

GLOSARIO

Código de activación

Es una clave única que se puede comprar al por menor y se utiliza para activar un producto o servicio específico. Un código de activación permite la activación de una suscripción válida por un cierto período de tiempo y número de dispositivos y también se puede utilizar para extender una suscripción con la condición de generarse para el mismo producto o servicio.

ActiveX

ActiveX es un modelo para escribir programas para que otros programas y el sistema operativo puedan llamarlos. La tecnología ActiveX se usa con Microsoft Internet Explorer para crear páginas web interactivas que se ven y se comportan como programas de computadora, en lugar de páginas estáticas. Con ActiveX, los usuarios pueden hacer o responder preguntas, usar botones e interactuar de otras formas con la página web. Los controles ActiveX a menudo se escriben usando Visual Basic. Active X se destaca por una completa falta de controles de seguridad; los expertos en seguridad informática desaconsejan su uso a través de internet.

Amenaza Persistente Avanzada

La amenaza persistente avanzada (APT) explota las vulnerabilidades de los sistemas para robar información importante y entregarla a la fuente. Grandes grupos, como organizaciones, empresas o gobiernos, son el blanco de esta amenaza. El objetivo de una amenaza persistente avanzada es pasar desapercibida durante mucho tiempo y poder monitorear y recopilar información importante sin dañar las máquinas objetivo. El método utilizado para inyectar la amenaza en la red es a través de un archivo PDF o un documento de Office que parezca inofensivo para que cada usuario pueda ejecutar los archivos.

publicidad

El adware a menudo se combina con una aplicación host que se proporciona sin cargo siempre que el usuario acepte el adware. Debido a que las aplicaciones de adware generalmente se instalan después de que el usuario haya aceptado un acuerdo de licencia que establece el propósito de la aplicación, no se comete ningún delito. Sin embargo, los anuncios emergentes pueden convertirse en una molestia y, en algunos casos,

degradar el rendimiento del sistema. Además, la información que recopilan algunas de estas aplicaciones puede causar problemas de privacidad para los usuarios que no conocían completamente los términos del acuerdo de licencia.

Archivo

Disco, cinta o directorio conteniendo ficheros almacenados.

Un archivo que contiene uno o más archivos en un formato comprimido.

Puerta trasera

Un agujero en la seguridad de un sistema dejado deliberadamente por diseñadores o mantenedores. La motivación de tales agujeros no siempre es siniestra; algunos sistemas operativos, por ejemplo, vienen listos para usar con cuentas privilegiadas destinadas a los técnicos de servicio de campo o los programadores de mantenimiento del proveedor.

Sector de arranque

Un sector al comienzo de cada disco que identifica la arquitectura del disco (tamaño del sector, tamaño del clúster, etc.). Para los discos de inicio, el sector de arranque también contiene un programa que carga el sistema operativo.

virus de arranque

Una amenaza que infecta el sector de arranque de un disco fijo o disquete. Un intento de arrancar desde un disquete infectado con un virus del sector de arranque hará que la amenaza se active en la memoria. Cada vez que inicie su sistema a partir de ese momento, tendrá la amenaza activa en la memoria.

red de bots

El término “botnet” se compone de las palabras “robot” y “red”. Los botnets son dispositivos conectados a Internet infectados con amenazas y se pueden usar para enviar correos electrónicos no deseados, robar datos, controlar de forma remota dispositivos vulnerables o propagar spyware, ransomware y otros tipos de amenazas. Su objetivo es infectar el mayor número posible de dispositivos conectados, como PC, servidores, dispositivos móviles o IoT pertenecientes a grandes empresas o industrias.

Navegador

Abreviatura de navegador web, una aplicación de software utilizada para localizar y mostrar páginas web. Los navegadores populares incluyen Microsoft Internet Explorer, Mozilla Firefox y Google Chrome. Estos son navegadores gráficos, lo que significa que pueden mostrar gráficos además de texto. Además, la mayoría de los navegadores modernos pueden presentar información multimedia, incluidos sonido y video, aunque requieren complementos para algunos formatos.

Ataque de fuerza bruta

Ataque de adivinación de contraseñas utilizado para ingresar en un sistema informático ingresando posibles combinaciones de contraseñas, en su mayoría comenzando con la contraseña más fácil de adivinar.

Línea de comando

En una interfaz de línea de comandos, el usuario escribe los comandos en el espacio provisto directamente en la pantalla usando el lenguaje de comandos.

Galletas

Dentro de la industria de Internet, las cookies se describen como pequeños archivos que contienen información sobre computadoras individuales que los anunciantes pueden analizar y usar para rastrear sus intereses y gustos en línea. En este ámbito, la tecnología de cookies aún se está desarrollando y la intención es orientar los anuncios directamente a lo que ha dicho que son sus intereses. Es un arma de doble filo para muchas personas porque, por un lado, es eficiente y pertinente, ya que solo ve anuncios sobre lo que le interesa. Por otro lado, implica realmente "rastrear" y "seguir" a dónde va y lo que haces clic. Comprensiblemente, existe un debate sobre la privacidad y muchas personas se sienten ofendidas por la noción de que se les considera un "número SKU" (ya sabe, el código de barras en la parte posterior de los paquetes que se escanea en la línea de pago del supermercado) . Si bien este punto de vista puede ser extremo, en algunos casos es exacto.

Ciberacoso

Cuando compañeros o extraños están cometiendo actos abusivos contra los niños con el propósito de lastimarlos físicamente. Para dañar emocionalmente, los agresores envían mensajes crueles o fotos poco favorecedoras, lo que hace que sus víctimas se aíslen de los demás o se sientan frustradas.

Ataque de diccionario

Los ataques de adivinación de contraseñas solían entrar en un sistema informático ingresando una combinación de palabras comunes para generar posibles contraseñas. El mismo método se utiliza para adivinar las claves de descifrado de mensajes o documentos cifrados. Los ataques de diccionario tienen éxito porque muchas personas se inclinan por elegir contraseñas cortas y de una sola palabra que sean fáciles de adivinar.

Disco duro

Es una máquina que lee y escribe datos en un disco. Una unidad de disco duro lee y escribe discos duros. Una unidad de disquete accede a disquetes. Las unidades de disco pueden ser internas (alojadas dentro de una computadora) o externas (alojadas en una caja separada que se conecta a la computadora).

Descargar

Para copiar datos (generalmente un archivo completo) desde una fuente principal a un dispositivo periférico. El término se usa a menudo para describir el proceso de copiar un archivo de un servicio en línea a la propia computadora. Descargar también puede referirse a copiar un archivo desde un servidor de archivos de red a una computadora en la red.

Correo electrónico

Correo electrónico. Un servicio que envía mensajes en computadoras a través de redes locales o globales.

Eventos

Una acción u ocurrencia detectada por un programa. Los eventos pueden ser acciones del usuario, como hacer clic con el botón del mouse o presionar una tecla, o eventos del sistema, como quedarse sin memoria.

hazañas

Una forma de aprovechar diferentes errores o vulnerabilidades que están presentes en una computadora (software o hardware). Por lo tanto, los piratas informáticos pueden obtener el control de las computadoras o las redes.

Falso positivo

Ocurre cuando un escáner identifica un archivo como infectado cuando en realidad no lo está.

Extensión de nombre de archivo

La parte de un nombre de archivo, después del punto final, que indica el tipo de datos almacenados en el archivo. Muchos sistemas operativos utilizan extensiones de nombre de archivo, por ejemplo, Unix, VMS y MS-DOS. Por lo general, tienen de una a tres letras (algunos sistemas operativos tristes y antiguos no admiten más de tres). Los ejemplos incluyen "c" para código fuente C, "ps" para PostScript, "txt" para texto arbitrario.

Heurístico

Un método basado en reglas para identificar nuevas amenazas. Este método de escaneo no se basa en una base de datos de información de amenazas específica. La ventaja del análisis heurístico es que no se deja engañar por una nueva variante de una amenaza existente. Sin embargo, ocasionalmente puede reportar código sospechoso en programas normales, generando el llamado "falso positivo".

Tarro de miel

Un sistema informático de señuelo configurado para atraer a los piratas informáticos para que estudien la forma en que actúan e identifiquen los métodos heréticos que utilizan para recopilar información del sistema. Las empresas y corporaciones están más interesadas en implementar y utilizar trampas trampa para mejorar su estado general de seguridad.

IP

Protocolo de Internet: un protocolo enrutable en el conjunto de protocolos TCP/IP que es responsable del direccionamiento IP, el enrutamiento y la fragmentación y reensamblaje de paquetes IP.

Subprograma de Java

Un programa Java que está diseñado para ejecutarse solo en una página web. Para usar un subprograma en una página web, debe especificar el nombre del subprograma y el tamaño (largo y ancho, en píxeles) que puede utilizar el subprograma. Cuando se accede a la página web, el navegador descarga el applet de un servidor y lo ejecuta en la máquina del usuario (el cliente). Los applets se diferencian de las aplicaciones en que se rigen por un estricto protocolo de seguridad.

Por ejemplo, aunque los subprogramas se ejecutan en el cliente, no pueden leer ni escribir datos en la máquina del cliente. Además, los subprogramas están más restringidos para que solo puedan leer y escribir datos del mismo dominio desde el que se sirven.

registrador de teclas

Un keylogger es una aplicación que registra todo lo que escribes. Los keyloggers no son de naturaleza maliciosa. Se pueden usar para fines legítimos, como monitorear la actividad de los empleados o los niños. Sin embargo, los ciberdelincuentes los utilizan cada vez más con fines maliciosos (por ejemplo, para recopilar datos privados, como credenciales de inicio de sesión y números de seguridad social).

Virus de macros

Un tipo de amenaza informática que se codifica como una macro incrustada en un documento. Muchas aplicaciones, como Microsoft Word y Excel, admiten potentes lenguajes de macros. Estas aplicaciones le permiten incrustar una macro en un documento y hacer que la macro se ejecute cada vez que se abre el documento.

cliente de correo

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

Memoria

Áreas de almacenamiento interno en la computadora. El término memoria identifica el almacenamiento de datos que viene en forma de chips, y la palabra almacenamiento se usa para la memoria que existe en cintas o discos. Cada computadora viene con una cierta cantidad de memoria física, generalmente denominada memoria principal o RAM.

no heurístico

Este método de escaneo se basa en una base de datos de información de amenazas específicas. La ventaja del análisis no heurístico es que no se deja engañar por lo que podría parecer una amenaza y no genera falsas alarmas.

Depredadores en línea

Individuos que buscan atraer a menores o adolescentes a conversaciones con el propósito de involucrarlos en actividades sexuales ilegales. Las redes sociales son el lugar ideal donde los niños vulnerables pueden ser perseguidos y seducidos fácilmente para que cometan actividades sexuales, en línea o cara a cara.

Programas empaquetados

Un archivo en un formato de compresión. Muchos sistemas operativos y aplicaciones contienen comandos que le permiten empaquetar un archivo para que ocupe menos memoria. Por ejemplo, suponga que tiene un archivo de texto que contiene diez caracteres de espacio consecutivos. Normalmente, esto requeriría diez bytes de almacenamiento.

Sin embargo, un programa que empaqueta archivos reemplazaría los caracteres de espacio por un carácter de serie de espacio especial seguido por la cantidad de espacios que se reemplazan. En este caso, los diez espacios requerirían solo dos bytes. Esta es solo una técnica de empaque, hay muchas más.

Camino

Las direcciones exactas a un archivo en una computadora. Estas direcciones generalmente se describen mediante el sistema de archivo jerárquico de arriba hacia abajo.

La ruta entre dos puntos, como el canal de comunicación entre dos computadoras.

Suplantación de identidad

El acto de enviar un correo electrónico a un usuario que afirma falsamente ser una empresa legítima establecida en un intento de estafar al usuario para que entregue información privada que se utilizará para el robo de identidad. El correo electrónico dirige al usuario a visitar un sitio web donde se le pide que actualice la información personal, como contraseñas y números de tarjetas de crédito, seguridad social y cuentas bancarias, que ya tiene la organización legítima. El sitio web, sin embargo, es falso y está configurado solo para robar la información del usuario.

Fotón

Photon es una innovadora tecnología no intrusiva de Bitdefender, diseñada para minimizar el impacto en el rendimiento de su solución de seguridad. Al monitorear la actividad de su PC en segundo plano, crea patrones de uso que ayudan a optimizar los procesos de arranque y escaneo.

Virus polimórfico

Una amenaza que cambia de forma con cada archivo que infecta. Como no tienen un patrón binario constante, estas amenazas son difíciles de identificar.

Puerto

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

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

Ransomware

El ransomware es un programa malicioso que trata de obtener dinero de los usuarios mediante el bloqueo de sus sistemas vulnerables. Cryptolocker, CryptoWall y TeslaWall son solo algunas de las variantes que secuestran los sistemas personales de los usuarios.

La infección puede propagarse al acceder a spam, descargar archivos adjuntos, o instalar aplicaciones, evitando que el usuario se percate de lo que está sucediendo en su sistema. Los usuarios habituales y empresas son el objetivo de los hackers de ransomware.

Archivo de informe

Es un fichero que lista las acciones realizadas. BitDefender genera un archivo de informe (log) que contiene una lista de las rutas analizadas, las carpetas, el número de archivos y archivos comprimidos analizados, el número de archivos infectados y sospechosos que se han detectado.

Rootkit

Un rootkit es un conjunto de herramientas de software que ofrecen acceso al sistema a nivel de administrador. El término empezó a usarse con los sistemas operativos UNIX y se refería a las herramientas que proporcionaban permisos de administrador a los intrusos, permitiéndoles ocultar su presencia para no ser vistos por los administradores de sistema.

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

Rootkits no son de naturaleza mala. Por ejemplo, los sistemas y algunas aplicaciones esconden ficheros críticos usando rootkits. No obstante, se usan habitualmente para ocultar amenazas o para encubrir la presencia

de un intruso en el sistema. Cuando se combinan con amenazas, los rootkits representan un gran peligro para la integridad y la seguridad de un sistema. Pueden monitorizar el tráfico, crear puertas traseras en el sistema, alterar ficheros y logs y evitar su detección.

Script

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

Spam

Correo basura o posts basura en grupos de noticias. Se conoce generalmente como correo no deseado.

Spyware

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

La similitud del spyware con una amenaza de tipo troyano radica en el hecho de que los usuarios instalan involuntariamente el producto al instalar otra cosa. Una forma habitual de infectarse con spyware es descargando, a través de programas de intercambio de ficheros, un determinado archivo que intercambia el nombre de los productos compartidos.

A parte de las cuestiones de ética y privacidad, el spyware roba al usuario recursos de memoria y ancho de banda mientras envía la información al creador del spyware a través de la conexión de Internet del usuario. Puesto que el spyware utiliza memoria y recursos del sistema, las aplicaciones que se ejecutan en segundo plano pueden provocar errores del sistema o inestabilidad general del mismo.

Elementos de inicio

Todos los ficheros de esta carpeta se abren al iniciar el ordenador. Por ejemplo, una pantalla de inicio, un archivo de sonido para que se

reproduzca cuando se inicie el equipo, un calendario de recordatorios o apps pueden ser elementos de inicio. Normalmente, se elige un alias del fichero para ubicar en esta carpeta y no directamente el fichero.

Suscripción

Acuerdo de compra que otorga al usuario el derecho a utilizar un producto o servicio determinado en un número concreto de dispositivos y durante cierto periodo de tiempo. Una suscripción caducada puede renovarse automáticamente utilizando la información proporcionada por el usuario en su primera compra.

Bandeja del sistema

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

TCP/IP

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

Amenaza

Es un programa o una parte de un código cargado en su ordenador sin avisarle y en contra de su voluntad. La mayoría de las amenazas también pueden autorreplicarse. Todas las amenazas informáticas están creadas por el hombre. Una amenaza sencilla que pueda copiarse una y otra vez es relativamente fácil de producir. Incluso una amenaza tan simple es peligrosa porque consumirá rápidamente toda la memoria disponible y hará que el sistema se detenga. Un tipo de amenaza aún más peligrosa es la capaz de transmitirse a través de las redes y eludir los sistemas de seguridad.

Actualización de información sobre amenazas

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

Troyano

Es un programa destructivo disfrazado como aplicación benigna. A diferencia de los programas de software malicioso y gusanos, los troyanos no se autorreplican, pero pueden ser igualmente destructivos. Uno de los tipos de troyanos más graves es una amenaza que pretende desinfectar su equipo, pero en cambio introduce amenazas en él.

El término tiene origen en la famosa obra "La Ilíada" de Homero, en la cual Grecia entrega un gigantesco caballo de madera a sus enemigos, los Troyanos, como supuesta oferta de paz. Pero una vez los Troyanos arrastraron el caballo hasta el interior de las murallas de la ciudad, los soldados Griegos salieron de un hueco del vientre del caballo y abrieron las puertas de las murallas, permitiendo la entrada de sus compatriotas y la conquista de Troya.

Actualizar

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

Bitdefender posee una característica de actualización que le permite comprobar manualmente las actualizaciones o actualizar automáticamente el producto.

Red privada virtual (VPN)

Es una tecnología que permite una conexión directa temporal y cifrada a una determinada red a través de una red menos segura. De esta forma, el envío y recepción de datos está cifrado y es seguro, lo que dificulta su intercepción por parte de los fisgones. Una muestra de seguridad es la autenticación, que solo se puede lograr utilizando un nombre de usuario y contraseña.

Gusano

Un programa que se autopropaga a través de una red, reproduciéndose a medida que avanza. No puede adjuntarse a otros programas.