Bitdefender®
ANTIVIRUS FOR MAC

GUÍA DE USUARIO

Mac

Bitdefender Antivirus for Mac

Guía de usuario

Fecha de publicación 24/11/2022

Aviso Legal

Bitdefender

Tabla de contenidos

ACERCA DE ESTA GUÍA

Propósito y público al que va dirigida

Esta guía está dirigida a todos los usuarios Macintosh que han elegido Bitdefender Antivirus for Mac como solución de seguridad para sus ordenadores personales. La información presentada en este libro es apta no sólo para expertos en informática, sino para todo aquel capaz de trabajar bajo Macintosh.

Averiguará cómo configurar y usar Bitdefender Antivirus for Mac para protegerse contra amenazas y otro software malicioso. Descubrirá cómo sacar el máximo partido de su Bitdefender.

Le deseamos una útil y placentera lectura.

Cómo usar esta guía

Esta guía está organizada en diversos temas principales:

Iniciando (página 11)

Comience con Bitdefender Antivirus for Mac y su interfaz de usuario.

Protección contra Software Malicioso (página 15)

Aprenda a como utilizar Bitdefender Antivirus for Mac para protegerse contra software malicioso.

Preferencias de Configuración (página 36)

Aprenda más sobre las preferencias de Bitdefender Antivirus for Mac.

Obteniendo ayuda (página 54)

Dónde consultar y dónde pedir ayuda si se produce una situación inesperada.

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. QUÉ ES BITDEFENDER ANTIVIRUS FOR MAC

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

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

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

2. INSTALACIÓN Y DESINSTALACIÓN

Este capítulo incluye los siguientes temas:

2.1. Requisitos del sistema

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

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

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

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

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

2.2. Instalación de Bitdefender Antivirus for Mac

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

1. Inicie sesión como administrador.
2. Ir a: https://central.bitdefender.com.
3. Inicie sesión en su cuenta de Bitdefender con su dirección de correo electrónico y contraseña.

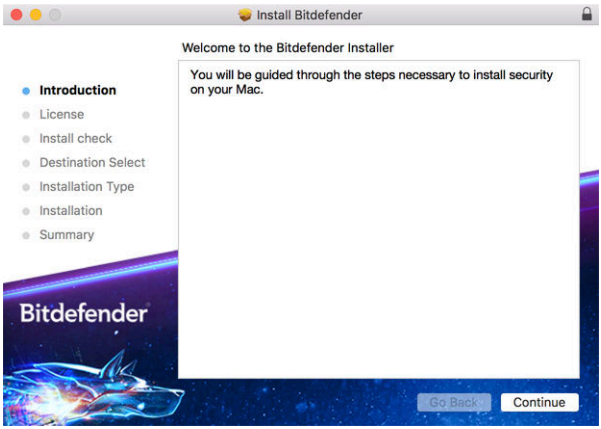
4. Seleccione el panel **Mis dispositivos** y, a continuación, toque **INSTALAR PROTECCIÓN**.
5. Escoja una de las dos opciones disponibles:
   - **Proteger este dispositivo**
     a. Seleccione esta opción y, a continuación, seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
     b. Guarde el archivo de instalación.
   - **Proteger otros dispositivos**
     a. Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
     b. Toque **ENVIAR ENLACE DE DESCARGA**.
     c. Introduzca una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR CORREO ELECTRÓNICO**.
     Tenga en cuenta que el enlace de descarga generado solo es válido durante las próximas 24 horas. Si caducase, debería generar uno nuevo siguiendo los mismos pasos.
     d. En el dispositivo en que desee instalar su producto Bitdefender, compruebe la cuenta de correo electrónico que introdujo y luego haga clic en el botón de descarga correspondiente.
6. Ejecute el producto Bitdefender que ha descargado.
7. Siga los pasos de la instalación.

2.2.1. Proceso de instalación

Para instalar Bitdefender Antivirus for Mac:

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

Paso 1 - Ventana de Bienvenida



Haga clic en **Continuar**.

Paso 2: Lea el Acuerdo de Suscripción

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

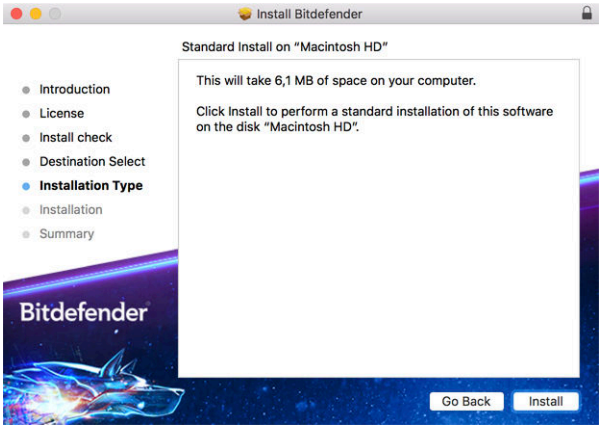
Desde esta ventana también puede seleccionar el idioma en el que desea instalar el producto.

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

Importante

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

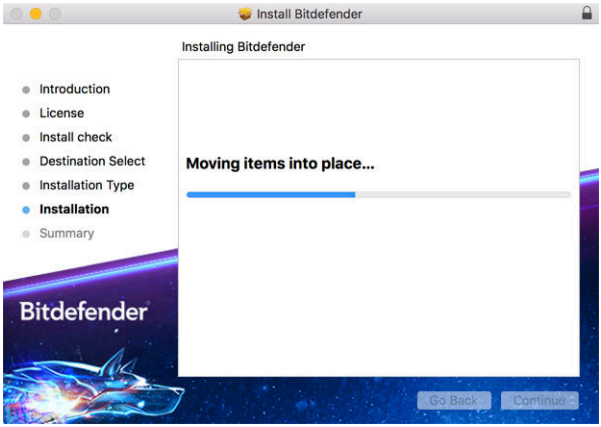
Paso 3 - Iniciar la instalación



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

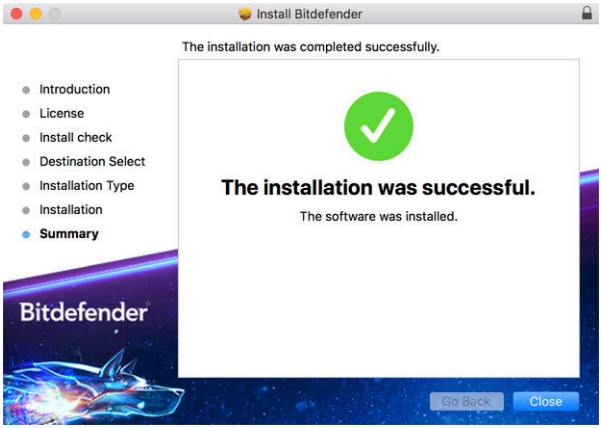
Haga clic en **Instalar** para iniciar la instalación.

Paso 4 - Instalando Bitdefender Antivirus for Mac



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

Paso 5 - Finalizar



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

Ha finalizado el proceso de instalación.

Importante

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

2.3. Desinstalando Bitdefender Antivirus for Mac

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

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

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

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

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

   Importante
   Si hay un error, puede contactar con Atención al Cliente de Bitdefender como se describe en Solicitando Ayuda (página 54).

3. INICIANDO

Este capítulo incluye los siguientes temas:

3.1. Abriendo Bitdefender Antivirus for Mac

Hay diferentes maneras de abrir Bitdefender Antivirus for Mac.

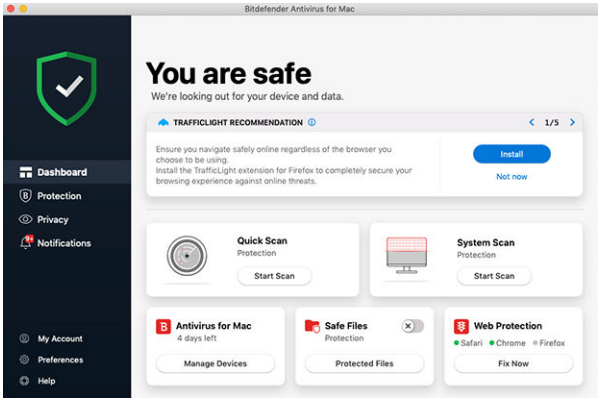
- Haga clic en el icono Bitdefender Antivirus for Mac en el Launchpad.
- Haga clic en el icono de la barra de menús y seleccione **Abrir interfaz antivirus**.
- Abra una ventana del Finder, acceda a Aplicaciones y haga doble clic en el icono **Bitdefender Antivirus for Mac**.

> **Importante**
> La primera vez que abra Bitdefender Antivirus for Mac en macOS Mojave 10.14 o en una versión más reciente, aparecerá una recomendación de protección porque necesitamos permisos para analizar todo el sistema en busca de amenazas. Para otorgarnos dichos permisos, debe iniciar sesión como administrador y seguir los pasos que se exponen a continuación:
>
> 1. Haga clic en el enlace **Preferencias del sistema**.
> 2. Haga clic en el icono y, a continuación, introduzca sus credenciales de administrador.
> 3. Se abre una nueva ventana. Arrastre el archivo **BDLDaemon** a la lista de apps permitidas.

3.2. Ventana principal de la app

Bitdefender Antivirus for Mac satisface las necesidades tanto de los usuarios más técnicos como de los usuarios principiantes. Esta interfaz

de usuario gráfica esta diseñada para satisfacer todas y cada una de las categorías de usuario.



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

La barra de estado en la parte superior de la ventana le informa sobre el estado de seguridad del sistema mediante mensajes explícitos y colores asociados. Si Bitdefender Antivirus for Mac carece de avisos, la barra de estado es verde. Cuando se detecta un problema de seguridad, la barra de estado se pone roja. Para obtener información detallada sobre cualquier problema y cómo solucionarlo, consulte Reparar Incidencias (página 27).

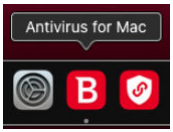
Para ofrecerle un funcionamiento eficaz y una mayor protección mientras lleva a cabo diferentes actividades, el **Autopilot de Bitdefender** actuará como su asesor de seguridad personal. Dependiendo de la actividad que realice, ya esté trabajando o haciendo pagos por Internet, el Autopilot de Bitdefender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

Desde el menú de navegación del lado izquierdo, puede acceder a las secciones de Bitdefender para una configuración detallada y tareas administrativas avanzadas (pestañas **Protección** y **Privacidad**),

notificaciones, su **cuenta de Bitdefender** y el área de **Preferencias**. Además, puede ponerse en contacto con nosotros (pestaña **Ayuda**) para obtener ayuda en caso de tener alguna pregunta o si sucede algo inesperado.

3.3. Icono de app del Dock

El icono de Bitdefender Antivirus for Mac puede verse en el Dock en cuanto abre la aplicación. El icono del Dock le proporciona una manera fácil para analizar archivos y carpetas en busca de amenazas. Simplemente arrastre y suelte el archivo o la carpeta en el icono del Dock y el análisis comenzará inmediatamente.



3.4. Menú de navegación

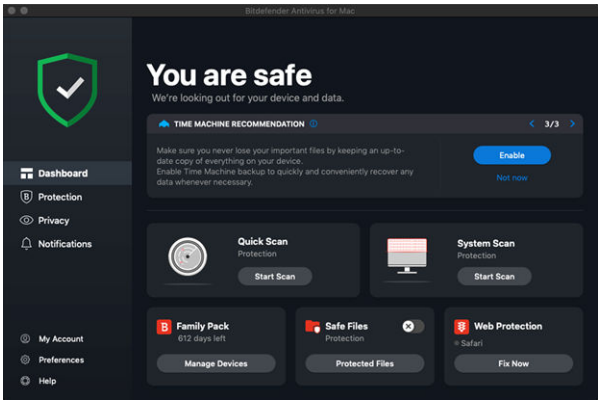
En el lado izquierdo de la interfaz de Bitdefender está el menú de navegación, que le permite acceder rápidamente a las características de Bitdefender que necesita para gestionar su producto. Las pestañas disponibles en esta área son las siguientes:

- **Panel de control**. Desde aquí puede solucionar rápidamente los problemas de seguridad, ver recomendaciones según las necesidades de su sistema y sus patrones de uso, realizar acciones rápidas y acceder a su cuenta de Bitdefender para administrar los dispositivos que ha añadido a su suscripción de Bitdefender.
- **Protección**. Desde aquí puede poner en marcha análisis antivirus, añadir archivos a la lista de excepciones, proteger archivos y aplicaciones frente a ataques de ransomware, salvaguardar sus copias de seguridad de Time Machine y configurar su protección mientras navega por Internet.
- **Privacidad**. Desde aquí, puede abrir la aplicación Bitdefender VPN e instalar la extensión Anti-tracker en su navegador.
- **Notificaciones**. Desde aquí puede ver detalles sobre las acciones realizadas en los archivos analizados.

- **Mi Cuenta**. Desde aquí, puede ver la cuenta de Bitdefender y la suscripción que protege a su dispositivo, además de cambiar su cuenta, en caso necesario.
- **Preferencias**. Desde aquí puede configurar los ajustes de Bitdefender.
- **Ayuda**. Desde aquí, siempre que necesite ayuda para resolver cualquier incidencia con su producto de Bitdefender, puede ponerse en contacto con el servicio de soporte técnico. También puede enviarnos sus comentarios para ayudarnos a mejorar el producto.

3.5. Modo oscuro

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



4. PROTECCIÓN CONTRA SOFTWARE MALICIOSO

Este capítulo incluye los siguientes temas:

4.1. Mejores Prácticas

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

- Mantenga habilitado **Bitdefender Residente**, para permitir que Bitdefender Antivirus for Mac analice automáticamente los archivos del sistema.
- Mantenga Bitdefender Antivirus for Mac actualizado con la última información de amenazas y actualizaciones de producto.
- Compruebe y repare regularmente las incidencias reportadas por Bitdefender Antivirus for Mac. Para información detallada, diríjase a Reparar Incidencias (página 27).
- Verifique el registro detallado de eventos relativos a la actividad de Bitdefender Antivirus for Mac en su equipo. Siempre que sucede algo relevante para la seguridad de su sistema o de sus datos, se añade

un nuevo mensaje al área de notificaciones de Bitdefender. Para más información, acceda a Notificaciones (página 28).

- También debería seguir estas recomendaciones:
  - Acostúmbrese a analizar los archivos que descargue de una fuente de almacenamiento externa (como por ejemplo una memoria USB o un CD), especialmente cuando desconoce el origen de los mismos.
  - Si tiene un archivo DMG, móntelo y analice su contenido (los archivos del volumen/imagen montado).

  La manera más fácil de analizar un archivo, una carpeta o un disco es arrastrarlos y soltarlos en la ventana de Bitdefender Antivirus for Mac o sobre el icono del Dock.

No se requiere otra acción o configuración. Sin embargo, si lo desea, puede ajustar la configuración de la aplicación y las preferencias para satisfacer mejor sus necesidades. Para más información, diríjase a Preferencias de Configuración (página 36).

4.2. Analizando Su Mac

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

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

También puede iniciar un análisis de la siguiente manera:

1. Haga clic en **Protección** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Antivirus**.
3. Haga clic en uno de los tres botones de análisis para iniciar el análisis deseado.
   - **Quick Scan:** busca amenazas en las ubicaciones más vulnerables de su sistema (por ejemplo, las carpetas que contienen los

documentos, descargas, descargas de correo electrónico y archivos temporales de cada usuario).

- **Análisis del sistema:** Realiza una comprobación exhaustiva en busca de amenazas en todo el sistema. Todos los dispositivos montados se analizarán también.

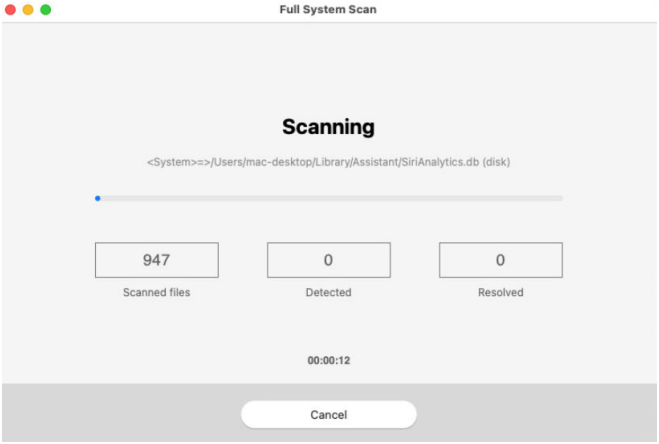
  > **Nota**
  > Dependiendo del tamaño de su disco duro, analizar todo el sistema puede tardar bastante (hasta una hora o incluso más). Para mejorar el rendimiento, se recomienda no ejecutar esta tarea mientras se estén llevando a cabo otras tareas que consuman muchos recursos (como por ejemplo la edición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

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

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

4.3. Asistente del Análisis

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



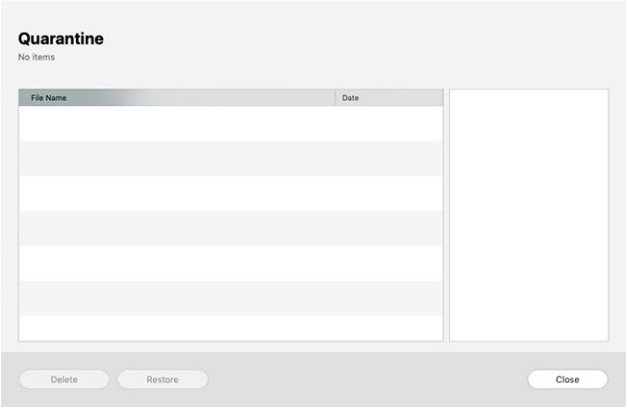
Durante cada análisis se muestra Información en tiempo real acerca de las amenazas detectadas y resueltas.

Espere a que Bitdefender Antivirus for Mac finalice el análisis.

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

4.4. Cuarentena

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



El apartado Cuarentena muestra todos los archivos actualmente aislados en la carpeta Cuarentena.

Para borrar un archivo de la cuarentena, selecciónelo y haga clic en **Eliminar**. Si desea restaurar una archivo en cuarentena a su ubicación original, selecciónelo y haga clic en **Restaurar**.

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

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

4.5. Bitdefender Residente (protección en tiempo real)

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

Para desactivar la protección en tiempo real:

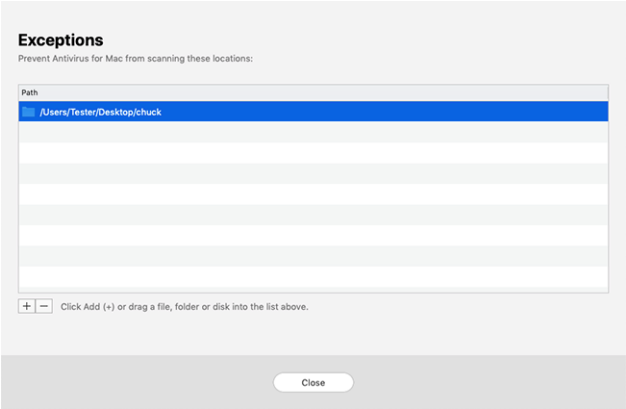
1. Haga clic en **Preferencias** en el menú de navegación de la interfaz de Bitdefender.
2. Desactive **Bitdefender Residente** en la ventana **Protección**.

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

4.6. Excepciones al análisis

Si así lo desea, puede hacer que Bitdefender Antivirus for Mac no analice ciertos archivos, carpetas o incluso un volumen entero. Por ejemplo, quizá querría excluir del análisis:

- Archivos que han sido identificados por error como infectados (conocidos como falsos positivos)
- Archivos que provocan errores de análisis
- Hacer copia de seguridad de los volúmenes



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

Para acceder a la lista de excepciones:

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

Existen dos modos de establecer una excepción de análisis:

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

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

4.7. Protección Web

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

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

4.7.1. Habilitación de extensiones Traffic Light

Para habilitar las extensiones de TrafficLight:

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

4.7.2. Ajustes de administración de extensiones

Hay toda una serie de funciones disponibles para protegerle frente a todo tipo de amenazas que pueda encontrar mientras navega por la Web. Para acceder a ellos, haga clic en el icono TrafficLight junto a la configuración de su navegador y, a continuación, haga clic en el botón **Ajustes**:

- **Ajustes de Bitdefender Traffic Light**
  - Protección web: Evita que acceda a sitios web empleados para ataques de phishing, fraudes y malware.
  - Asesor de búsquedas: Proporciona una advertencia anticipada sobre sitios web peligrosos presentes en sus resultados de búsquedas.

- **Excepciones**
  Si se encuentra en el sitio web que desea añadir a las excepciones, haga clic en **Añadir el sitio web actual a la lista**.
  Si desea añadir otro sitio web, escriba su dirección en el campo correspondiente y, a continuación, haga clic en .
  No se mostrará ninguna advertencia en caso de que haya amenazas en las páginas exceptuadas. Por eso solo debería añadir a esta lista sitios web en los que confíe plenamente.

4.7.3. Calificación de páginas y alertas

Dependiendo de la clasificación que TrafficLight otorgue a la página Web que esté viendo, mostrará en su área uno de los iconos siguientes:

Esta es una página segura. Puede seguir trabajando.

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

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

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

4.8. Anti-tracker

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

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

La extensión de Bitdefender es compatible con los siguientes navegadores:

- Google Chrome
- Mozilla Firefox
- Safari

Los rastreadores que detectamos se agrupan en las siguientes categorías:

- **Publicidad:** Se utilizan para analizar el tráfico del sitio web, el comportamiento de los usuarios o los patrones de tráfico de los visitantes.

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

4.8.1. Activación de Bitdefender Anti-tracker

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

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

4.8.2. Interfaz de Anti-tracker

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

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

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

4.8.3. Desactivación de Bitdefender Anti-tracker

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

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

4.8.4. Permitir el rastreo de un sitio web

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

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

4.9. Safe Files

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

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

Para añadir posteriormente archivos al entorno protegido:

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

Para evitar que el sistema se ralentice, le recomendamos que añada un máximo de treinta carpetas, o que guarde varios archivos en una sola carpeta.

Las carpetas Imágenes, Documentos, Escritorio y Descargas están protegidas por defecto contra los ataques.

> **Nota**
> Se pueden proteger carpetas personalizadas solo para los usuarios actuales. No se pueden añadir al entorno de protección discos externos, archivos de aplicaciones y del sistema.

Se le informará cada vez que una aplicación desconocida con un comportamiento inusual intente modificar los archivos que ha añadido. Haga clic en **Permitir** o **Bloquear** para añadirlo a la lista de **Aplicaciones administradas**.

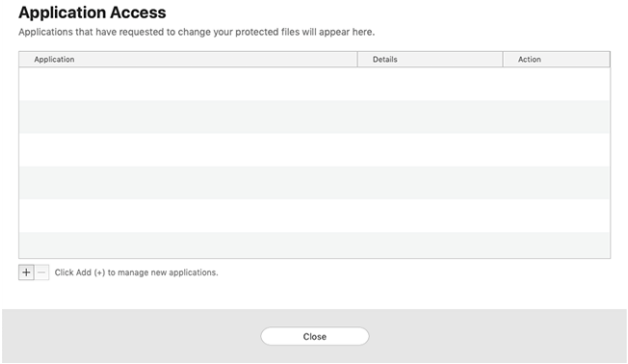
4.9.1. Acceso a las aplicaciones

Puede que las aplicaciones que intenten cambiar o borrar archivos protegidos se identifiquen como potencialmente poco fiables y se añadan a la lista de aplicaciones bloqueadas. Si se bloquease una aplicación y estuviese seguro de que su comportamiento es el adecuado, puede permitirla siguiendo estos pasos:

1. Hacer clic **Proteccion** en el menú de navegación de la interfaz de Bitdefender.
2. Selecciona el **Anti-ransomware** pestaña.
3. Haga clic en **Acceso a aplicaciones** en el área de Archivos seguros.
4. Cambie el estado a Permitir junto a la aplicación bloqueada.

Las aplicaciones fijadas en Permitir también se pueden pasar a estado Bloqueado.

Utilice el método de arrastrar y soltar o haga clic en el signo más (+) para añadir más apps a la lista.



4.10. Protección de Time Machine

La Protección de Time Machine de Bitdefender actúa como una capa adicional de seguridad para su unidad de copia de seguridad, incluyendo todos los archivos que haya decidido almacenar en ella, al bloquear el acceso desde cualquier fuente externa. En caso de que un ransomware cifrara los archivos que tiene almacenados en su unidad de Time Machine, podría recuperarlos sin tener que pagar el rescate solicitado.

En caso de que necesite restaurar elementos de una copia de seguridad de Time Machine, consulte la página de soporte técnico de Apple para obtener instrucciones.

4.10.1. Activación y desactivación de la Protección de Time Machine

Para activar o desactivar la Protección de Time Machine:

1. Haga clic en **Protección** en el menú de navegación de la **interfaz de Bitdefender**.
2. Selecciona el **Anti-ransomware** pestaña.
3. Active o desactive el conmutador de **Protección de Time Machine**.

4.11. Reparar Incidencias

Bitdefender Antivirus for Mac automáticamente detecta y le informa sobre una serie de incidencias que pueden afectar a la seguridad de su sistema y sus datos. De esta forma, puede evitar fácilmente y a tiempo riesgos para la seguridad.

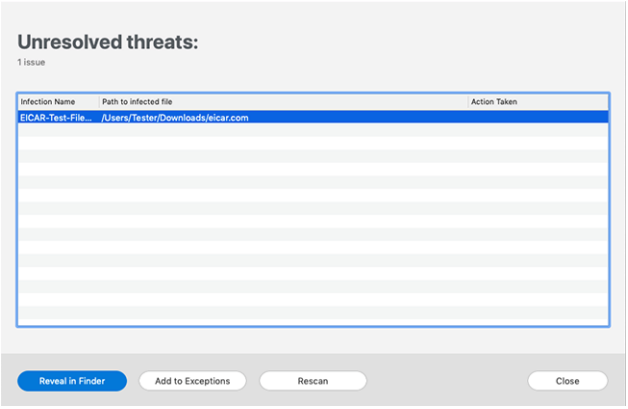
La reparación de incidencias indicadas por Bitdefender Antivirus for Mac es una manera rápida y sencilla de asegurarse una magnífica protección de su sistema y de sus datos.

Los problemas detectados incluyen:

- No se ha descargado de nuestros servidores la nueva actualización de la información de amenazas.
- Se han detectado amenazas en su sistema y el producto no puede desinfectarlas automáticamente.
- La protección en tiempo real está desactivada.

Para comprobar y reparar las incidencias detectadas:

1. Si Bitdefender no tiene avisos que presentar, la barra de estado es verde. Cuando se detecta un problema de seguridad, la barra de estado se pone roja.
2. Compruebe la descripción para más información.
3. Si se detecta un problema, haga clic en el botón correspondiente para adoptar medidas.



La lista de amenazas no resueltas se actualiza tras cada análisis del sistema, independientemente de si el análisis se ha realizado automáticamente en segundo plano o si lo ha iniciado usted.

Puede escoger adoptar las siguientes medidas respecto a las amenazas no solucionadas:

- **Eliminar manualmente.** Lleve a cabo esta acción para eliminar manualmente las infecciones.
- **Añadir a excepciones.** Esta acción no está disponible para amenazas encontradas dentro de archivos comprimidos.

4.12. Notificaciones

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

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

Para acceder al registro de notificaciones, haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender. Cada vez que se produce un evento crítico, se puede ver un contador en el icono 2.

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

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

Haga clic en cada pestaña para obtener más información sobre los eventos generados. Con un simple clic en el título de cada evento se muestran algunos detalles: una breve descripción, la medida que

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

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

4.13. Actualizaciones

Todos los días se encuentran e identifican nuevas amenazas. Por este motivo es muy importante mantener Bitdefender Antivirus for Mac al día con las últimas actualizaciones de información de amenazas.

La actualización de información de amenazas se realiza al instante, reemplazándose progresivamente los archivos que haya que actualizar. De este modo, la actualización no afecta al funcionamiento del producto y, al mismo tiempo, se evita cualquier riesgo.

- Si Bitdefender Antivirus for Mac está actualizado, este puede detectar las últimas amenazas descubiertas y limpiar los archivos infectados.
- Si Bitdefender Antivirus for Mac no está actualizado, no podrá detectar y eliminar las últimas amenazas descubiertas por los laboratorios de Bitdefender.

4.13.1. Solicitando una Actualización

Puede solicitar una actualización manualmente en cualquier momento.

Se requiere conexión a Internet con el fin de comprobar las actualizaciones disponibles y descargarlas.

Para solicitar una actualización manual:

1. Haga clic en el botón **Acciones** en la barra de menús.
2. Elija **Actualizar la base de datos de información de amenazas**.

Como alternativa, puede solicitar manualmente una actualización pulsando CMD + U.

Puede ver el progreso de actualización y archivos descargados.

4.13.2. Obteniendo Actualizaciones a través de un Servidor Proxy

Bitdefender Antivirus for Mac se puede actualizar solo a través de servidores proxy que no requieran autenticación. No tiene que configurar ningún ajuste de programa.

Si se conecta a Internet a través de un servidor proxy que requiera autenticación, debe pasar regularmente a una conexión directa a Internet para obtener actualizaciones de la información de amenazas.

4.13.3. Actualice a una nueva versión

De vez en cuando, lanzamos actualizaciones de producto para añadir nuevas características y mejoras o solucionar deficiencias del producto. Estas actualizaciones podrían requerir un reinicio del sistema para dar paso a la instalación de nuevos archivos. De forma predeterminada, si una actualización precisa un reinicio del equipo, Bitdefender Antivirus for Mac seguirá funcionando con los archivos anteriores hasta que se reinicie el sistema. Así, el proceso de actualización no interferirá con el trabajo del usuario.

Cuando se complete una actualización del producto, una ventana emergente le informará de que debe reiniciar el sistema. Si no lee esta notificación, puede también hacer clic en **Reiniciar para actualizar** en la barra de menús o reiniciar manualmente el sistema.

4.13.4. Hallar información sobre Bitdefender Antivirus for Mac

Para hallar información sobre la versión de Bitdefender Antivirus for Mac que ha instalado, acceda a la ventana **Acerca de**. En la misma ventana, puede acceder al Acuerdo de suscripción, la Política de privacidad y las Licencias de código abierto y leer estos documentos.

Para acceder a la ventana Acerca de:

1. Abrir Bitdefender Antivirus for Mac.
2. En la barra de menús, haga clic en Bitdefender Antivirus for Mac y elija **Acerca de Antivirus for Mac**.

5. VPN

Este capítulo incluye los siguientes temas:

5.1. Acerca de VPN

Con Bitdefender VPN puede mantener la privacidad de sus datos personales cada vez que se conecta a redes inalámbricas inseguras de aeropuertos, centros comerciales, cafeterías u hoteles. De esta forma, se pueden evitar situaciones desafortunadas como el robo de datos personales o que piratas informáticos intenten acceder a la dirección IP de su dispositivo.

Puede instalar la aplicación VPN desde su producto Bitdefender y usarla cada vez que desee añadir una capa más de protección a su conexión. La VPN actúa como túnel entre su dispositivo y la red a la que se conecta, para proteger su conexión, cifrar los datos mediante algoritmos de nivel bancario y ocultar su dirección IP dondequiera que esté. Su tráfico se redirige a través de un servidor independiente, lo que hace que su dispositivo sea casi imposible de identificar entre la infinidad de dispositivos que utilizan nuestros servicios. Además, mientras está conectado a Internet a través de Bitdefender VPN, puede acceder a contenidos que normalmente están restringidos en determinadas zonas.

Nota

Algunos países practican la censura de Internet y, por lo tanto, el uso de las VPN en su territorio está prohibido por la ley. Para evitar responsabilidades legales, puede que aparezca un mensaje de advertencia cuando trate de utilizar la app VPN por primera vez. Al seguir haciendo uso de esa app, confirma que es consciente de las regulaciones nacionales aplicables y de los riesgos a los que podría exponerse.

5.2. Abrir VPN

Hay tres formas de abrir la aplicación de Bitdefender VPN:

- Haga clic en **Privacidad** en el menú de navegación de la **interfaz de Bitdefender**.
  Haga clic en **Abrir** en la tarjeta de Bitdefender VPN.
- Haga clic en el icono de la barra de menú.
- Acceda a la carpeta Aplicaciones, abra la carpeta Bitdefender y, a continuación, haga doble clic en el icono de Bitdefender VPN.

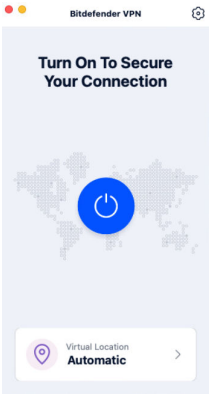
La primera vez que abra la aplicación, se le pedirá permiso para que Bitdefender añada configuraciones. Al permitir que Bitdefender añada configuraciones, acepta que toda la actividad de red de su dispositivo se podrá filtrar o monitorizar cuando use la aplicación de VPN.

> **Nota**
> La aplicación Bitdefender VPN solo se puede instalar en macOS Sierra (10.12.6), macOS High Sierra (10.13.6) o macOS Mojave (10.14) o versiones posteriores del sistema operativo.

5.3. Interfaz

La interfaz de VPN muestra el estado de la app: conectada o desconectada. Para los usuarios con la versión gratuita, Bitdefender configura automáticamente la ubicación del servidor a la más apropiada, mientras que los usuarios Premium tienen la posibilidad de cambiar la ubicación del servidor al que deseen conectarse escogiéndola en la lista Ubicaciones virtuales. Para más información sobre las suscripciones a VPN, consulte Suscripciones (página 34).

Para conectarse o desconectarse, basta con hacer clic en el estado que se muestra en la parte superior de la pantalla. El icono de la barra de menú aparece en negro cuando VPN está conectado y en blanco cuando no.



Mientras está conectado, el tiempo transcurrido se muestra en la parte inferior de la interfaz. Para acceder a más opciones, haga clic en el icono ⚙ de la zona superior derecha:

- **Mi cuenta:** Se muestran los detalles sobre su cuenta de Bitdefender y su suscripción a VPN. Haga clic en **Cambiar cuenta** si desea iniciar sesión con otra distinta.
- **Ajustes:** Puede personalizar el comportamiento de su producto según sus necesidades:
  - **General**
    - Notificaciones: Muestra las notificaciones del producto.
    - Ejecutar en el arranque: Lanza automáticamente Bitdefender VPN al iniciar sesión.
    - Informes del producto: Envía informes anónimos del producto para ayudarnos a mejorar su experiencia y su capacidad de protección.
  - **Avanzado**
    - Conmutador de interrupción de Internet: Interrumpe temporalmente todo el tráfico de Internet si se suspende la conexión VPN.
    - Bloqueador de anuncios y Anti-tracker: Bloquea anuncios y rastreadores para disfrutar de una web más limpia y rápida.
    - Túnel dividido: Los sitios web seleccionados se saltarán la VPN y accederán directamente a Internet.

> **Nota**
> Haga clic en **Administrar** y, a continuación, en **Añadir sitio web** para añadir páginas web a esta lista.

- Conexión automática: Conecta la VPN automáticamente en los siguientes casos:
  - Conexión a una red Wi-Fi pública o insegura.
  - Se inicia una aplicación de intercambio de archivos punto a punto.

- **Soporte técnico:** Se le redirige a la plataforma de nuestro centro de soporte, donde puede leer un artículo sobre cómo usar Bitdefender VPN.
- **Acerca de:** Muestra información sobre la versión instalada.
- **Salir:** Sale de la aplicación.

5.4. Suscripciones

Bitdefender VPN ofrece de forma gratuita una cuota diaria de tráfico de 200 MB por dispositivo para proteger la conexión cada vez que lo necesite y le conecta automáticamente a la ubicación del servidor óptimo.

Para disfrutar de tráfico y acceso ilimitado a contenidos en todo el mundo y elegir la ubicación del servidor que desee, actualice a la versión premium.

Puede actualizar a la versión Bitdefender Premium VPN en cualquier momento tocando el botón **Actualizar** disponible en la interfaz del producto.

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

Bitdefender VPN es un producto multiplataforma, disponible en los productos Bitdefender compatibles con Windows, macOS, Android y iOS.

Una vez que actualice al plan Premium, podrá usar su suscripción en todos los productos, siempre que inicie sesión con la misma cuenta de Bitdefender.

6. PREFERENCIAS DE CONFIGURACIÓN

Este capítulo incluye los siguientes temas:

6.1. Preferencias de Acceso

Para abrir la ventana de Preferencias de Bitdefender Antivirus for Mac:

- Realice una de estas acciones:
  - Hacer clic **preferencias** en el menú de navegación de la interfaz de Bitdefender.
  - Haga clic en la barra de menú de Bitdefender Antivirus for Mac y escoja **Preferencias**.

6.2. Preferencias de protección

La ventana de preferencias de protección le permite configurar el procedimiento general de análisis. Puede configurar las acciones a realizar en los archivos infectados y sospechosos detectados y otros ajustes generales.

- **Bitdefender Residente.** Bitdefender Residente brinda protección en tiempo real contra un amplio abanico de amenazas mediante el análisis de todas las aplicaciones instaladas, sus versiones actualizadas y archivos nuevos y modificados. Le recomendamos que no desactive Bitdefender Residente pero, en caso necesario, hágalo durante el menor tiempo posible. Si desactiva el Bitdefender Residente, no estará protegido contra las amenazas.
- **Analizar solo archivos nuevos y modificados.** Marque esta casilla de verificación para que Bitdefender Antivirus for Mac analice solo los archivos que no se han analizado antes o que se han modificado desde su último análisis.

Puede optar por no aplicar este ajuste al análisis personalizado y al de arrastrar y soltar dejando sin marcar la casilla de verificación correspondiente.

- **No analizar el contenido de las copias de seguridad.** Marque esta casilla de verificación para excluir del análisis los archivos de copia de seguridad. Si posteriormente se restauran los archivos infectados, Bitdefender Antivirus for Mac los detectará automáticamente y adoptará las medidas oportunas.

6.3. Preferencias avanzadas

Puede elegir una acción general para todas las incidencias y elementos sospechosos hallados durante un proceso de análisis.

Acción para elementos infectados

- **Intentar desinfectar o mover a la cuarentena:** Si se detectan archivos infectados, Bitdefender intentará desinfectarlos (eliminando el código malicioso).
- **No realizar ninguna acción:** No se realizará ninguna acción sobre los archivos detectados.

Acción para elementos sospechosos

- **Mover archivos a la cuarentena:** Si se detectan archivos sospechosos, Bitdefender los moverá a la cuarentena.
- **No tomar ninguna medida** - No se realizará ninguna acción sobre los archivos detectados.

6.4. Ofertas especiales

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

Para activar o desactivar las notificaciones de ofertas especiales:

1. Hacer clic **preferencias** en el menú de navegación de la interfaz de Bitdefender.
2. Seleccione la pestaña **Otros**.

3. Active o desactive el conmutador **Mis ofertas**.

> **Nota**
> La opción **Mis ofertas** está habilitada por defecto.

7. 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:
  - Bitdefender Antivirus para Mac
  - La línea de productos de Windows de Bitdefender
  - 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.

7.1. Acceso a Bitdefender Central

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

- Desde la interfaz principal de Bitdefender Antivirus for Mac:

1. Haga clic en el enlace **Ir a su cuenta** de la parte inferior derecha de la pantalla.

- Desde su navegador Web:
  1. Abra un navegador Web en cualquier dispositivo con acceso a internet.
  2. 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.

7.2. Autenticación en dos fases

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

7.2.1. Activar la autenticación en dos fases

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

Para habilitar la autenticación en dos fases:

1. Acceda a **Bitdefender Central**.
2. 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. 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**.

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.

7.3. 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.

7.4. 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.

7.4.1. Añadir un nuevo dispositivo

Si su suscripción cubre más de un dispositivo, puede añadir un nuevo dispositivo e instalarle Bitdefender Antivirus for Mac 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.

7.4.2. 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**.

7.4.3. 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.

7.5. 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.

7.6. Mis suscripciones

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

7.6.1. 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).

7.6.2. 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.

7.6.3. 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.

7.7. 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.

8. PREGUNTAS FRECUENTES

¿Cómo puedo probar Bitdefender Antivirus for Mac antes de solicitar una suscripción?

Es un nuevo cliente de Bitdefender y le gustaría probar nuestro producto antes de comprarlo. El periodo de evaluación es de treinta días y puede seguir utilizando el producto instalado con solo adquirir una suscripción de Bitdefender. Para probar Bitdefender Antivirus for Mac, tiene que:

1. Crear una cuenta Bitdefender siguiendo estos pasos:
   a. Ir a: https://central.bitdefender.com.
   b. Escriba la información requerida en los campos correspondientes. Los datos que proporcione aquí serán confidenciales.
   c. Antes de seguir adelante, debe aceptar los Términos de uso. Acceda a los Términos de uso y léalos detenidamente, ya que contienen los términos y condiciones bajo los cuales puede usar Bitdefender.
   Además, puede acceder a la Política de privacidad y leerla.
   d. Haga clic en **CREAR CUENTA**.
2. Descargue Bitdefender Antivirus for Mac de la siguiente manera:
   a. Selecciona el **Mis dispositivos** panel y, a continuación, haga clic en **INSTALAR PROTECCIÓN**.
   b. Elija una de las dos opciones disponibles:
      - **Protege este dispositivo**
        i. Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
        ii. Guarde el archivo de instalación.
      - **Proteger otros dispositivos**
        i. Seleccione esta opción y luego seleccione el propietario del dispositivo. Si el dispositivo pertenece a otra persona, haga clic en el botón correspondiente.
        ii. Hacer clic **ENVIAR ENLACE DE DESCARGA**.

iii. Escriba una dirección de correo electrónico en el campo correspondiente y haga clic en **ENVIAR CORREO ELECTRÓNICO**.

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

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

c. Ejecute el producto Bitdefender que ha descargado.

Tengo un código de activación. ¿Cómo puedo añadir su validez a mi suscripción?

Si compró un código de activación de uno de nuestros revendedores o lo recibió como regalo, puede agregar su disponibilidad a su suscripción de Bitdefender.

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

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

La extensión se puede ver ahora en su cuenta Bitdefender, y en su producto Bitdefender Antivirus for Mac instalado, en la parte inferior derecha de la pantalla.

El registro de análisis indica que todavía hay elementos sin resolver. ¿Cómo los elimino?

Los elementos sin resolver en el registro de análisis pueden ser:

- archivos de acceso restringido (xar, rar, etc.)
  Solución: Utilice la opción **Mostrar en el Finder** para encontrar el archivo y borrarlo manualmente. Asegúrese de vaciar la Papelera.

- buzones de correo de acceso restringido (Thunderbird, etc.)
  Solución: Utilice la aplicación para eliminar la entrada que contiene el archivo infectado.
- Contenido de las copias de seguridad
  Solución: Activar la opción **No analizar el contenido de las copias de seguridad** en Preferencias de protección o **Añadir a excepciones** los archivos detectados.
  Si posteriormente se restauran los archivos infectados, Bitdefender Antivirus for Mac los detectará automáticamente y adoptará las medidas oportunas.

> **Nota**
> Se entiende por archivos de acceso restringido aquellos que Bitdefender Antivirus for Mac solo puede abrir, pero no puede modificar.

¿Dónde puedo leer información detallada sobre la actividad del producto?

Bitdefender mantiene un registro de todas las acciones importantes, cambios de estado y otros mensajes críticos relacionados con su actividad. Para acceder a esta información, haga clic en **Notificaciones** en el menú de navegación de la interfaz de Bitdefender.

¿Puedo actualizar Bitdefender Antivirus for Mac a través de un servidor proxy?

Bitdefender Antivirus for Mac puede actualizarse solo a través de servidores proxy que no requieren autenticación. No tiene que configurar ningún ajuste del programa.

Si se conecta a Internet a través de un servidor proxy que requiere autenticación, debe cambiar periódicamente a una conexión directa a Internet para obtener actualizaciones de información sobre amenazas.

¿Cómo desinstalo Bitdefender Antivirus for Mac?

Para eliminar Bitdefender Antivirus for Mac, siga estos pasos:

1. Abra una ventana del **Finder** y luego acceda a la carpeta Aplicaciones.
2. Abra la carpeta Bitdefender y, a continuación, haga doble clic en BitdefenderUninstaller.
3. Hacer clic **Desinstalar** y esperar a que se complete el proceso.

4. Hacer clic **Cerca** para terminar.

> **Importante**
> Si hay un error, puede ponerse en contacto con Atención al cliente de Bitdefender como se describe en Solicitando Ayuda (página 54).

¿Cómo elimino las extensiones TrafficLight de mi navegador?

- Para eliminar las extensiones TrafficLight de Mozilla Firefox, siga los pasos siguientes:
  1. Acceda a **Herramientas** y seleccione **Complementos**.
  2. Seleccione **Extensiones** en la columna izquierda.
  3. Seleccione las extensiones y haga clic en **Eliminar**.
  4. Reinicie el navegador para completar el proceso de eliminación.

- Para eliminar las extensiones TrafficLight de Google Chrome, siga los pasos siguientes:
  1. En la parte superior derecha, haga clic en **Más** ⋮.
  2. Acceda a **Más herramientas** y seleccione **Extensiones**.
  3. Haga clic en el icono **Eliminar** 🗑 junto a la extensión que desea eliminar.
  4. Haga clic en **Eliminar** para confirmar el proceso de eliminación.

- Para eliminar las extensiones Traffic Light de Safari, siga los pasos siguientes:
  1. Acceda a **Preferencias** o pulse **Comando-Coma (,)**.
  2. Seleccione **Extensiones**.
     Se mostrará una lista con las extensiones instaladas.
  3. Seleccione la extensión Bitdefender Traffic Light y, a continuación, haga clic en **Quitar**.
  4. Haga clic en **Quitar** para confirmar el proceso de eliminación.

¿Cuándo debo usar Bitdefender VPN?

Debe tener cuidado cuando acceda, descargue o cargue contenidos en internet. Para asegurarse de que se mantiene a salvo mientras navega por la web, le recomendamos que use Bitdefender VPN cuando:

- Desee conectarse a redes inalámbricas públicas.
- Desee acceder a contenidos que normalmente están restringidos en zonas concretas, sin importar si está en su hogar o en el extranjero.
- Desee mantener la privacidad de sus datos personales (nombres de usuario, contraseñas, información de tarjetas de crédito, etc.).
- Desee ocultar su dirección IP.

¿Afecta negativamente Bitdefender VPN a la duración de la batería de mi dispositivo?

Bitdefender VPN está diseñado para proteger sus datos personales, ocultar su dirección IP mientras está conectado a redes inalámbricas inseguras y acceder a contenidos restringidos en ciertos países. Para evitar el consumo innecesario de la batería de su dispositivo, le recomendamos que use VPN solo cuando lo necesite, y que prescinda de él cuando no esté conectado.

¿Por qué parece ir más lento Internet cuando me conecto a través de Bitdefender VPN?

Bitdefender VPN está pensado para brindarle agilidad cuando navega por la web; sin embargo, su conectividad a Internet o la distancia al servidor con el que se conecta pueden producir demoras. De ser así, si no es imprescindible que se conecte desde su ubicación a un servidor lejano (por ejemplo, desde Estados Unidos hasta China), le recomendamos que permita que Bitdefender VPN le conecte automáticamente al servidor más cercano o que encuentre un servidor más próximo a su ubicación actual.

9. OBTENIENDO AYUDA

9.1. 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.

9.2. 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.

9.2.1. 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/.

9.2.2. 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

9.2.3. 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/.

9.3. 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 54).

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

9.3.1. 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.