GUÍA DE USUARIO

Bitdefender CONSUMER SOLUTIONS

VPN

Bitdefender VPN

Guía de Usuario

Publication date 02/07/2024

Advertencia legal

Bitdefender

Tabla de contenidos

ACERCA DE ESTA GUÍA

Propósito y público al que se dirige

Esta guía va dirigida a todos los usuarios de Bitdefender que hayan elegido Bitdefender VPN como servicio de referencia para disfrutar del anonimato online mediante el cifrado de todo el tráfico entrante y saliente de su PC, Mac o dispositivo móvil.

Averiguará cómo configurar y usar Bitdefender VPN para mantener su identidad y sus actividades online a salvo de los piratas informáticos. Aprenderá a sacarle el máximo partido a Bitdefender.

Le deseamos una lectura útil y agradable.

Cómo usar esta guía

Esta guía está organizada en diversos temas principales:

Qué es Bitdefender VPN (página 4)

Comience con Bitdefender VPN aprendiendo qué es y cómo puede ayudarle a protegerse otorgándole un verdadero anonimato online.

Uso de Bitdefender VPN (página 13)

Aprenda a interactuar con Bitdefender VPN y con su interfaz de usuario.

Ajustes y características de Bitdefender VPN (página 17)

Obtenga más información sobre los ajustes y funcionalidades de Bitdefender VPN.

Obteniendo ayuda (página 31)

Dónde buscar y dónde solicitar ayuda si surge algo inesperado.

Convenciones utilizadas en esta guía

Convenciones tipográficas

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

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

Advertencias

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

Nota

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

Importante

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

Advertencia

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

Solicitud de comentarios

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

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

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

1. QUÉ ES BITDEFENDER VPN

La VPN sirve como un túnel entre su dispositivo y la red a la que se conecta para proteger su conexión, cifrar los datos mediante cifrado de grado militar y ocultar su dirección IP dondequiera que esté. Su tráfico se redirige a través de un servidor independiente; lo que hace que sea imposible que su ISP identifique su dispositivo, a través de la gran cantidad de otros dispositivos que utilizan nuestros servicios. Además, mientras esté conectado a Internet a través de Bitdefender VPN, podrá acceder a contenido que normalmente está restringido en áreas específicas.

Nota

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

1.1. Protocolos de cifrado

A continuación se proporcionan los conjuntos de cifrado por defecto habilitados en el cliente y servidor Hydra. Los demás conjuntos de cifrado están inhabilitados.

Conjuntos de cifrado del cliente Hydra:

- ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-SHA:ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES128-SHA:ECDHE-RSA-AES256-SHA:DHE-RSA-AES128-SHA
- DHE-RSA-AES256-SHA:AES128-SHA:AES256-SHA:DES-CBC3-SHA

Nota

El conjunto del lado del servidor es mucho más restrictivo y tanto el cliente como el servidor Hydra rechazarán un modo que no sea GCM con AES. El servidor Hydra impone la prioridad de conjuntos de cifrado más fuertes del lado del servidor y rechazará el protocolo de enlace TLS si un cliente solicita un conjunto más débil. Esta lista también es configurable en tiempo de ejecución del lado del servidor.

2. SUSCRIPCIONES DE VPN

Con Bitdefender VPN, puede optar por dos tipos de suscripciones:

- Las suscripción básica
- La suscripción Premium

2.1. Suscripción básica

Bitdefender VPN ofrece de forma gratuita una cuota diaria de tráfico de 200 MB por dispositivo para proteger su conexión cuando lo necesite y le permite conectarse a una única ubicación que no se puede cambiar.

La suscripción básica está a disposición de cualquier usuario que descargue Bitdefender VPN.

2.2. Suscripción Premium

Para obtener acceso ilimitado a todas las características incluidas en Bitdefender VPN, actualice a la versión Premium. Los usuarios con una suscripción VPN Premium activa tienen tráfico protegido ilimitado y pueden conectarse a cualquiera de nuestros servidores en todo el mundo.

Hay dos planes disponibles para la suscripción Premium: mensual y anual.

- Plan mensual: con este plan, se le cobrará cada mes por los servicios Premium VPN. Puede anular su suscripción cuando lo desee.
- Plan anual: requiere un pago único que le otorga acceso a nuestros servicios Premium VPN durante todo un año.

2.3. Cómo actualizar a Premium VPN

La forma más fácil de actualizar a la versión Premium de Bitdefender VPN es hacer clic en el botón **Actualizar** ubicado en la parte inferior de la interfaz principal. Elija el modelo de suscripción deseado y luego siga las instrucciones que aparecen en la pantalla.

Si ya tiene un código de activación, siga las instrucciones que se exponen a continuación:

- **Para usuarios de Windows**

1. Haga clic en el icono Mi cuenta de la izquierda de la interfaz de VPN.
2. Haga clic en **Añadir aquí**.
3. Escriba el código recibido por correo electrónico y, a continuación, haga clic en el botón **Activar código**.

- **Para usuarios de macOS**
  1. Haga clic en el engranaje de la esquina superior derecha de la interfaz de VPN y seleccione **Mi cuenta**.
  2. Hacer clic **Agrégalo aquí**.
  3. Escriba el código recibido por correo electrónico, luego haga clic en el **codigo de activacion** botón.

- **Para usuarios de Android**
  1. Toque en el engranaje de la esquina superior derecha de la interfaz de VPN y seleccione **Mi cuenta**.
  2. Toque en **Añadir código**.
  3. Escriba el código recibido por correo electrónico, luego haga clic en el **codigo de activacion** botón.

- **Para usuarios de iOS**
  1. Toque la rueda dentada en la esquina superior derecha de la interfaz VPN y seleccione **Mi cuenta**.
  2. Grifo **Agregar código**.
  3. Escriba el código recibido por correo electrónico, luego haga clic en el **codigo de activacion** botón.

3. INSTALACIÓN

3.1. Preparándose para la instalación

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

- Asegúrese de que el dispositivo donde piensa instalar Bitdefender cumple los requisitos del sistema. Si el dispositivo no cumple con todos los requisitos del sistema, Bitdefender no se instalará o, si estuviera instalado, no funcionaría correctamente y provocaría demoras e inestabilidad en el sistema.
  Para ver la lista completa de todos los requisitos del sistema, consulte Requisitos del sistema (página 8)
- Inicie sesión en el dispositivo utilizando una cuenta de Administrador.
- Durante la instalación, se recomienda que su dispositivo esté conectado a Internet, incluso si la realiza desde un CD o DVD. Si hay disponibles versiones más recientes de los archivos de la aplicación incluidos en el paquete de instalación, Bitdefender puede descargarlas e instalarlas.

3.2. Requisitos del sistema

- **Para usuarios de Windows**
  - **Sistema operativo:** Windows 7 con Service Pack 1, Windows 8, Windows 8.1 Windows 10 y Windows 11
  - **Memoria (RAM):** 1 GB
  - **Espacio libre en disco:** 500 MB de espacio libre
  - **Net Framework:** versión mínima 4.5.2

    Importante
    El rendimiento del sistema puede verse afectado en dispositivos que tengan CPU de generaciones anteriores.
- **Para usuarios de macOS**
  - **Sistema operativo:** macOS Sierra (10.12) o posterior

- **Espacio libre en disco:** 100 MB de espacio libre

- **Para usuarios de Android**
  - **Sistema operativo:** Android 5.0 o posterior
  - **Almacenamiento:** 100 MB
  - Una conexión de Internet activa

- **Para usuarios de iOS**
  - **Sistema operativo:** iOS 12 o posterior
  - **Almacenamiento en iPhone:** 50 MB
  - **Almacenamiento en iPad:** 100 MB
  - Una conexión a Internet activa

3.3. Instalación de Bitdefender VPN

Para comenzar la instalación, siga las instrucciones correspondientes al sistema operativo que utilice:

- **Para usuarios de Windows**

  1. Para iniciar la instalación de Bitdefender VPN en un PC con Windows, empiece por descargar el kit de instalación desde https://www.bitdefender.com/solutions/vpn/download o desde el mensaje de correo electrónico que recibió tras realizar su compra.
  2. Haga doble clic en el instalador que ha descargado para ejecutarlo.
  3. Elija Sí si se le presenta el cuadro de diálogo del Control de cuentas de usuario.
  4. Espere a que se complete la descarga.
  5. Seleccione el idioma del producto utilizando el menú desplegable del instalador.
  6. Marque la casilla de verificación “Confirmo que he leído y acepto el Acuerdo de suscripción y la Política de privacidad” y, a continuación, haga clic en **INICIAR LA INSTALACIÓN**.
  7. Espere a que finalice la instalación.

8. **INICIE SESIÓN** con su cuenta de Bitdefender Central. Si carece de una cuenta de Central, regístrese para obtenerla haciendo clic en el botón **CREAR CUENTA**.
9. Elija **Tengo un código de activación** si ha comprado una suscripción Premium VPN.
   De lo contrario, puede elegir **COMENZAR LA EVALUACIÓN** para probar el producto de forma gratuita durante siete días antes de comprometerse a pagarlo.
10. Escriba el código recibido por correo electrónico y, a continuación, haga clic en el botón **ACTIVAR PREMIUM**.
11. Tras una corta espera, Bitdefender VPN queda instalado y listo para usarse en su equipo.

❍ **Para usuarios de macOS**

1. Para iniciar la instalación de Bitdefender VPN en macOS, empiece por descargar el kit de instalación desde https://www.bitdefender.com/solutions/vpn/download o desde el mensaje de correo electrónico que recibió tras realizar su compra.
2. El instalador se guardará en el Mac. En la carpeta Descargas, haga doble clic en el archivo de paquete de .
3. Siga las instrucciones que aparecen en la pantalla. Elija **Continuar**.
4. Se le guiará por los pasos necesarios para instalar Bitdefender VPN en su Mac. Haga clic dos veces en el botón **Continuar**.
5. Haga clic en **Aceptar** una vez leídos y aceptados los términos del acuerdo de licencia de software.
6. Haga clic en **Instalar**.
7. Introduzca un nombre de usuario y contraseña de administrador y, a continuación, haga clic en **Instalar el software**.
8. Se le notificará que se ha bloqueado una extensión de sistema firmada por Bitdefender. Esto no es un error, sino un mero control de seguridad. Haga clic en **Abrir preferencias de seguridad**.
9. Haga clic en el icono del candado para desbloquear.
   Introduzca un nombre y contraseña de administrador y, a continuación, pulse **Desbloquear**.

10. Haga clic en **Permitir** para cargar la extensión del sistema de BitdefenderBitdefender. Luego, cierre la ventana de Seguridad y privacidad y el instalador.

11. Acceda al icono del escudo en la barra de menús y, a continuación, **inicie sesión** con su cuenta de Bitdefender Central. Si carece de una cuenta de Central, regístrese para obtener una.

12. Elija tengo un **Código de activación** si ha comprado una suscripción Premium VPN.
    De lo contrario, puede elegir **INICIAR PRUEBA** para probar el producto de forma gratuita durante 7 días antes de comprometerse a pagarlo.

13. Escriba el código recibido por correo electrónico, luego haga clic en el **codigo de activacion** botón.

14. Tras una corta espera, Bitdefender VPN queda instalado y listo para usarse en su Mac.

❍ **Para usuarios de Android**

1. Para instalar Bitdefender VPN en Android, primero abra la aplicación **Google Play Store** en su smartphone o tablet.
2. Busque Bitdefender VPN y seleccione esta app.
3. Toque en el botón **Instalar** y espere a que se complete la descarga.
4. Toque en **Abrir** para ejecutar la app.
5. Marque la casilla de verificación “Acepto el Acuerdo de suscripción y la Política de privacidad” y, a continuación, toque en **Continuar**.
6. **Inicie sesión** con su cuenta de Bitdefender Central. Si carece de una cuenta de Central, regístrese para obtenerla tocando en **Crear cuenta**.
7. Elija **Tengo un código de activación** si ha comprado una suscripción Premium VPN.
   De lo contrario, puede elegir Iniciar la versión de evaluación gratuita de siete días para probar el producto antes de comprometerse a pagarlo.
8. Escriba el código recibido por correo electrónico y, a continuación, toque en **Activar código**.

- **Para usuarios de iOS**

  1. Para instalar Bitdefender VPN en iOS, primero abra la **App Store** en su iPhone o iPad.
  2. Buscar Bitdefender VPN y seleccione esta aplicación.
  3. Toque en el icono **Obtener** y espere a que se complete la descarga.
  4. Grifo **Abierto** para ejecutar la aplicación.
  5. Marque la casilla de verificación **Acepto el Acuerdo de suscripción y la Política de privacidad** y, a continuación, toque en **Continuar**.
  6. **Inicie sesión** con su cuenta de Bitdefender Central. Si carece de una cuenta, regístrese para obtenerla tocando en **Crear cuenta**.
  7. Toque en **Permitir** si desea recibir notificaciones de Bitdefender VPN.
  8. Elegir **tengo un codigo de activacion** si ha comprado una suscripción Premium VPN.
     De lo contrario, puede elegir Iniciar prueba de 7 días para probar el producto de forma gratuita durante 7 días antes de comprometerse a pagarlo.
  9. Escriba el código recibido por correo electrónico, luego toque **Codigo de activacion**.

4. USO DE BITDEFENDER VPN

4.1. Abrir Bitdefender VPN

- **Para Windows**
  Para acceder a la **interfaz principal de Bitdefender VPN**, utilice uno de los siguientes métodos:
  - **Desde la bandeja del sistema**
    Haga clic con el botón derecho en el ícono del escudo rojo de la bandeja del sistema y, a continuación, seleccione **Mostrar** en el menú.
  - **Desde la interfaz de Bitdefender**
    Si ya tiene instalado en su equipo con Windows algún producto de seguridad de Bitdefender, como Bitdefender Total Security o Bitdefender Antivirus Plus, puede abrir Bitdefender VPN desde allí:
    1. Haga clic en **Privacidad** en la barra lateral izquierda de la interfaz de Bitdefender.
    2. Haga clic en **Abrir VPN** en el panel de VPN.
  - **Desde su Escritorio**
    Haga doble clic en el acceso directo de Bitdefender VPN presente en su Escritorio.
- **Para macOS**
  Puede abrir la aplicación Bitdefender VPN haciendo clic en el icono de la barra de menús en la parte superior derecha de la pantalla.
  Si no encuentra el escudo de Bitdefender en la barra de menús, use el Launchpad o Finder de su Mac para recuperarlo:
  - **Desde Launchpad**
    1. Pulse **F4** en su teclado para entrar en el Launchpad de su Mac.
    2. Examine las páginas de las aplicaciones instaladas hasta que localice la de Bitdefender VPN. Como alternativa, puede escribir **Bitdefender VPN** en el Launchpad para filtrar sus resultados.
    3. Cuando haya localizado la aplicación Bitdefender VPN, haga clic en su icono para anclarlo a la barra de menús.

- **Desde Finder**

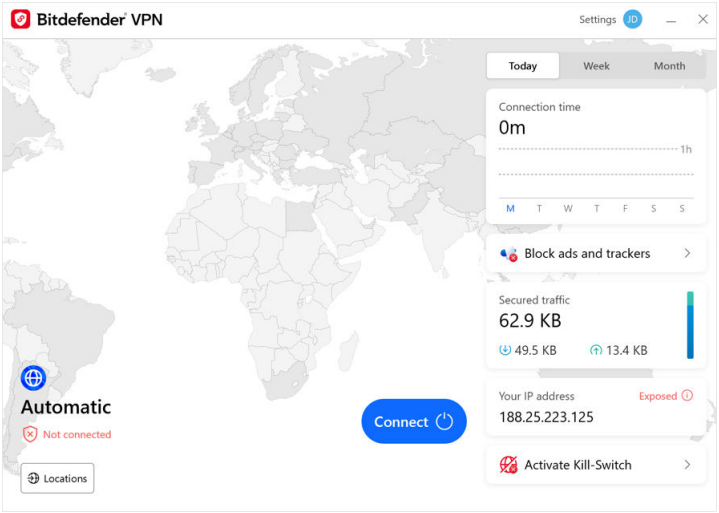
  1. Haga clic en **Finder** en la parte inferior izquierda del Dock (Finder es el icono del cuadrado azul con una cara sonriente).
  2. A continuación, haga clic en **Ir** en la parte superior izquierda de la pantalla, en la barra de menús.
  3. Seleccione **Aplicaciones** en el menú para acceder a la carpeta Aplicaciones de su Mac.
  4. Desde la carpeta Aplicaciones, abra la carpeta **Bitdefender** y, a continuación, haga doble clic en la aplicación de **Bitdefender VPN**.

Nota

Para acceder a Bitdefender VPN en sus dispositivos móviles Android o iOS, basta con que abra la aplicación Bitdefender VPN tras haberla instalado.

4.2. Cómo conectarse a Bitdefender VPN

La interfaz de VPN muestra el estado de la app: conectada o desconectada. Para los usuarios con la versión gratuita, Bitdefender configura automáticamente la ubicación del servidor a la más apropiada, mientras que los usuarios prémium tienen la posibilidad de cambiar la ubicación del servidor al que deseen conectarse escogiéndola en la lista de Ubicaciones virtuales. Para conectarse o desconectarse, haga clic en el botón de encendido de la interfaz de VPN.



- **Para Windows:** El icono del área de notificación muestra una marca de verificación verde cuando la VPN está conectada y una negra cuando no lo está. Mientras permanece conectado a una ubicación seleccionada manualmente, la interfaz principal muestra la dirección IP.
- **Para macOS:** El icono de la barra de menús aparece en negro cuando la VPN está conectada y en blanco cuando no lo está. Haga clic en el botón circular en medio de la interfaz y espere a que se establezca la conexión.
- **Para iOS y Android:** Para conectarse a Bitdefender VPN en iOS, iPadOS y Android, haga lo siguiente:
  - **En la app de Bitdefender VPN:** Para conectarse o desconectarse, toque el botón de encendido de la interfaz de VPN. Se muestra el estado de Bitdefender VPN.
  - **En la app Bitdefender Mobile Security:**
    1. Acceda al icono VPN en la barra de navegación inferior de Bitdefender Mobile Security.

2. Toque **CONECTAR** siempre que desee permanecer protegido mientras se conecte a redes inalámbricas inseguras. Toque **DESCONECTAR** cuando desee desactivar la conexión.

4.3. Cómo conectarse a un servidor diferente

Con una suscripción Premium, Bitdefender VPN le permite conectarse a cualquiera de nuestros servidores de todo el mundo en cualquier momento. Para ello, tendrá que hacer lo siguiente:

1. Abra la app Bitdefender VPN.
2. Toque en el botón **Ubicación virtual** de la zona inferior de la interfaz.
3. Seleccione el país que desee.
4. Haga clic en el botón **Conectarse a [país de su elección]** de la zona inferior de la interfaz.

- El icono de la bandeja del sistema muestra una marca de verificación verde cuando la VPN está conectada.
- La dirección IP del servidor virtual se muestra en la pantalla de inicio mientras está conectado a Bitdefender VPN.
- En el panel principal también se muestra un resumen de su tiempo de conexión, la cantidad de tráfico seguro y las últimas 5 ubicaciones a las que se conectó.

5. AJUSTES Y CARACTERÍSTICAS DE BITDEFENDER VPN

5.1. Acceso a los ajustes

Para acceder a los ajustes de Bitdefender VPN, deberá seguir los pasos que se describen a continuación:

- **En Windows**

  1. Abra la aplicación de Bitdefender VPN en su dispositivo haciendo doble clic en su icono en la bandeja del sistema o haciendo clic con el botón derecho sobre él y seleccionando Mostrar.
  2. Haga clic en el botón de **Ajustes** (representado por un engranaje) de la izquierda de la interfaz.

- **En macOS**

  1. Abra la aplicación de Bitdefender VPN en su dispositivo macOS haciendo clic en su icono en la barra de menús.
  2. Haga clic en el botón del engranaje de la esquina superior derecha de la interfaz de Bitdefender VPN y seleccione Ajustes.

- **En Android**

  1. Abra la aplicación de Bitdefender VPN en su dispositivo.
  2. Haga clic en el botón del engranaje de la esquina superior derecha de la interfaz de Bitdefender VPN.

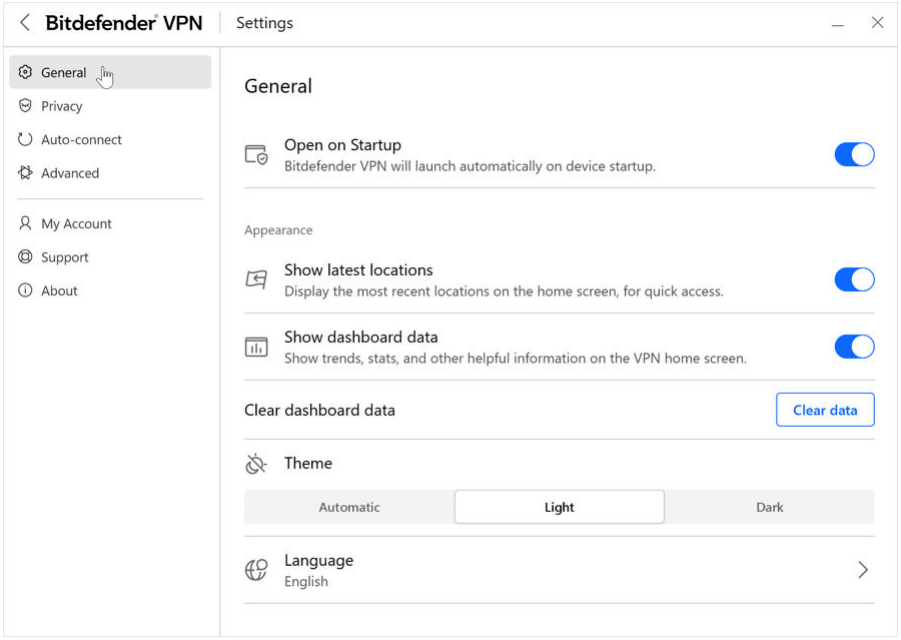
- **En iOS**

  1. Abre el Bitdefender VPN aplicación en su dispositivo.
  2. Haga clic en el botón de la rueda dentada en la esquina superior derecha de la Bitdefender VPN interfaz.

5.2. General

Aquí podrás modificar lo siguiente:

- **Abrir al iniciar**– Bitdefender VPN se iniciará automáticamente al iniciar el dispositivo.
- **Mostrar las últimas ubicaciones**– Muestra las ubicaciones más recientes en la pantalla de inicio, para un acceso rápido.
- **Mostrar datos del panel** – Muestra tendencias, estadísticas y otra información útil en la pantalla de inicio de VPN.
- **Borrar datos del panel**– Se borrarán todos los datos de su panel y se restablecerán todos los contadores.
- **Tema**– Tema claro/oscuro
- **Idioma**– Cambiar el idioma de Bitdefender VPN.
- **Notificaciones**– Administre sus preferencias de notificaciones.
- **Ayude a mejorar Bitdefender VPN**– Envíe informes anónimos de productos para ayudarnos a mejorar su experiencia.
- **Restablecer todos los ajustes**– Restablezca la VPN a su configuración original sin reinstalarla.



5.3. Características

5.3.1. Privacidad

Conmutador de interrupción de Internet

El conmutador de interrupción es una nueva característica implementada en Bitdefender VPN. Cuando está habilitada, esta característica interrumpe todo el tráfico de Internet si se suspende la conexión VPN. Tan pronto como vuelva a estar online, se restablecerá la conexión VPN.

Para activar el conmutador de interrupción, siga los pasos que se exponen a continuación:

- **en ventanas**

  1. Abra la aplicación de Bitdefender VPN en su dispositivo haciendo doble clic en su icono en la bandeja del sistema o haciendo clic con el botón derecho sobre él y seleccionando **Mostrar**.
  2. Clickea en el **Ajustes** botón (representado por una rueda dentada) en el lado izquierdo de la interfaz.
  3. Seleccione **Avanzado**.
  4. Habilite la opción **Conmutador de interrupción de Internet**.

- **En Android**

  1. Abre el Bitdefender VPN aplicación en su dispositivo.
  2. Haga clic en el botón de la rueda dentada en la esquina superior derecha de la Bitdefender VPN interfaz.
  3. En **Ajustes**, habilite la opción **Conmutador de interrupción**.

- **En iOS**

  1. Abre el Bitdefender VPN aplicación en su dispositivo.
  2. Haga clic en el botón de la rueda dentada en la esquina superior derecha de la Bitdefender VPN interfaz.
  3. Bajo **Ajustes**, habilitar el **Kill-Switch** opción.

> **Nota**
> Esta característica también está disponible para dispositivos macOS con sistemas operativos 10.15.4 o posteriores.

Bloqueador de anuncios y Anti-tracker

Estas características están pensadas para ayudarle a mantener la privacidad y disfrutar de la web sin molestos anuncios ni empresas que le vigilen. Ayudan a bloquear anuncios y detener rastreadores online.

Bloqueador de anuncios

El **Bloqueador de anuncios** se utiliza para bloquear anuncios, ventanas emergentes, anuncios de vídeo con sonido o banners publicitarios mientras navega. Esto contribuye a que los sitios web se carguen más rápidamente y se vean más despejados, además de resultar más seguro interactuar con ellos.

Para habilitar el Bloqueador de anuncios:

1. Localice la característica **Bloqueador de anuncios y Anti-tracker** en **Ajustes**.
2. Pase el conmutador a la posición **ACTIVADO**.

Anti-tracker

El **Anti-tracker** se utiliza para bloquear los rastreadores que los anunciantes configuran para seguirle y trazar su perfil online. Es posible que algunos sitios web no funcionen correctamente si se bloquean los rastreadores. Añadir su URL a la lista blanca podría solucionar este problema.

Para habilitar el Anti-tracker:

1. Localiza el **Bloqueador de anuncios y Antitracker** característica en **Ajustes**.
2. Cambie el interruptor a la **EN** posición.

Lista blanca

Es posible que algunos sitios web no se carguen correctamente si bloquea su código de rastreo y sus anuncios. Añadir las URL de estos dominios concretos a la lista blanca puede solucionar este problema, pero tenga

en cuenta que, mientras navegue por estos sitios web, verá anuncios y su código de rastreo permanecerá activo.

Añada el sitio web al que desea permitir mostrar anuncios y utilizar rastreadores de la siguiente manera:

1. Localiza el **Bloqueador de anuncios y Antitracker** característica en **Ajustes**.
2. Haga clic en el enlace **Administrar**. A continuación, acceda a la sección Lista blanca de la ventana y haga clic en el enlace **Administrar** correspondiente.
3. Haga clic en **Añadir sitio web** e introduzca la URL deseada.

5.3.2. Conectar automáticamente

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

Para protegerle de los peligros de los puntos de acceso inalámbricos públicos inseguros o sin cifrar, Bitdefender VPN incluye una característica de conexión automática. Esto significa que Bitdefender VPN puede activarse automáticamente en ciertas situaciones, dependiendo de sus preferencias y del sistema operativo en que se esté ejecutando.

- En **Windows**, la característica de conexión automática puede habilitarse en las siguientes situaciones:
  - **Inicio:** Conectar la VPN al inicio de Windows.
  - **Conexión Wi-Fi insegura:** Usar la VPN siempre que se conecte a redes Wi-Fi públicas o inseguras.
  - **Aplicaciones punto a punto:** Conectar la VPN cuando inicie una aplicación de uso compartido de archivos punto a punto.
  - **Aplicaciones y dominios:** Utilizar siempre la VPN para determinadas aplicaciones y sitios web.

Nota

1. Haga clic en el enlace **Administrar**.
2. Busque la ubicación de la aplicación para la que desea utilizar la VPN, seleccione su nombre y, a continuación, haga clic en **Añadir**.

- **Categorías de sitios web:** Conectar la VPN cuando visite determinadas categorías de sitios web. Bitdefender VPN puede conectarse automáticamente para las siguientes categorías de sitios web:
  - Finanzas
  - Pagos online
  - Salud
  - Intercambio de archivos
  - Citas Online
  - Contenido para adultos

Nota

Para cada categoría, puede seleccionar un servidor diferente al que se conecte la VPN.

- En **macOS**, la característica de conexión automática puede habilitarse en las siguientes situaciones:
  - **Inicio:** Conectar la VPN al inicio de macOS.
  - **Wi-Fi no seguro:** Utilice la VPN cada vez que se conecte a redes Wi-Fi públicas o no seguras.
  - **Aplicaciones punto a punto:** Conéctese a la VPN cuando inicie una aplicación para compartir archivos punto a punto.
  - **Aplicaciones:** Conectar siempre la VPN para determinadas aplicaciones.
- En **iOS** y **Android**, Bitdefender VPN puede configurarse para conectarse automáticamente solo cuando esté conectado a una red Wi-Fi pública o insegura.

5.3.3. Avanzado

Túnel dividido

El túnel dividido de red privada virtual (VPN) permite enrutar parte del tráfico de su aplicación o dispositivo a través de una VPN cifrada mientras que las otras aplicaciones o dispositivos acceden directamente a Internet. Esto es especialmente útil para beneficiarse de servicios que funcionan mejor cuando conocen su ubicación y, sin embargo, disfrutar de un acceso seguro a comunicaciones y datos potencialmente confidenciales.

Al habilitar la característica de **túnel dividido**, las aplicaciones y sitios web seleccionados se saltarán la VPN y accederán directamente a Internet.

Para administrar las aplicaciones y los sitios web que omiten la VPN, haga lo siguiente:

1. Haga clic en el enlace **Administrar** una vez que haya habilitado la característica.
2. Haga clic en el botón **Añadir**.
3. Busque la ubicación de la aplicación en cuestión o introduzca la URL del sitio web deseado y, a continuación, haga clic en **Añadir**.

> **Nota**
> Al añadir un sitio web, se omitirá el uso de VPN para todo el dominio, incluyendo sus subdominios.

> **Importante**
> En dispositivos **macOS**, la característica de túnel dividido solo se aplica a sitios web.

Optimizador de tráfico de aplicaciones

El Optimizador de tráfico de aplicaciones de Bitdefender VPN le permite dar prioridad al tráfico de las aplicaciones más importantes de su dispositivo sin exponer su conexión a riesgos para la privacidad. Las VPN redirigen el tráfico de Internet a través de un túnel seguro al tiempo que utilizan sólidos algoritmos de cifrado para protegerlo.

No obstante, esta combinación de técnicas puede acarrear algunos inconvenientes, principalmente en lo que se refiere a la velocidad de

conexión. Existen diversos factores que pueden ralentizar la conexión, como son la distancia al servidor al que se está conectando, la congestión de la red y el uso de un elevado ancho de banda. Si cree que, en ocasiones, Bitdefender VPN sobrecarga innecesariamente su conexión y le ocasiona demoras, puede que haya una solución mejor que desconectarse.

¿Cómo funciona el Optimizador de tráfico de aplicaciones?

Ciertas aplicaciones y servicios, como las plataformas de streaming, los clientes de torrent y los juegos, exigen más ancho de banda. Por ello, su uso constante podría afectar la velocidad de su conexión a Internet. Enrutar su tráfico a través de un túnel VPN ya somete su conexión a una relativa demora, de modo que tensionarla más podría degradar notablemente su experiencia online.

La característica Optimizador de tráfico de aplicaciones de Bitdefender VPN puede ayudarle a lidiar con las demoras de la conexión VPN dando prioridad a la aplicación que usted desee. Esta característica le permite decidir qué aplicaciones han de recibir la mayor parte del tráfico y, posteriormente, asigna los recursos en consecuencia. Por ejemplo, si se encuentra en una reunión y se da cuenta de que la calidad de la llamada no está a la altura, el Optimizador de tráfico de aplicaciones le permite priorizar el tráfico hacia la aplicación de videoconferencia para mejorar los resultados.

Normalmente, los usuarios de VPN recurrirían a cerrar todos los procesos que interfieran en su dispositivo o incluso a inhabilitar su conexión VPN para aumentar la velocidad de Internet. El Optimizador de tráfico de aplicaciones le permite disfrutar de una protección ininterrumpida de su privacidad sin comprometer por ello su velocidad de conexión.

Uso del Optimizador de tráfico de aplicaciones

Actualmente, esta característica solo está disponible en dispositivos Windows y le permite priorizar el tráfico de hasta tres aplicaciones.

Para habilitarla y configurarla con el mínimo esfuerzo, siga los pasos que se exponen a continuación:

1. Lance la aplicación Bitdefender VPN en su equipo con Windows.
2. Haga clic en el botón de la barra lateral para acceder a los ajustes de la VPN.

3. Acceda a la pestaña **General** y habilite la característica **Optimizador de tráfico de aplicaciones**. El color del conmutador pasará de gris a azul.

Para administrar las aplicaciones priorizadas por esta característica, haga lo siguiente:

1. Haga clic en el**Administrar**enlace.
2. Busque la ubicación de la aplicación para la que desea optimizar el tráfico, seleccione su nombre y, a continuación, haga clic en **Añadir**. La aplicación aparecerá en la sección **Con prioridad**.

> **Nota**
> Como alternativa, si ha abierto recientemente la aplicación que desea priorizar, pulse el botón + en la ventana del Optimizador de tráfico de aplicaciones.

3. Desconéctese y vuelva a conectarse a Bitdefender VPN tras añadir o eliminar aplicaciones de la lista.

Para eliminar una aplicación del Optimizador de tráfico de aplicaciones, basta con hacer clic en el icono junto a su nombre.

> **Nota**
> El Optimizador de tráfico de aplicaciones no está disponible en macOS.

Protocolo

Aquí puede elegir el tipo de protocolo que desea utilizar para la transferencia de datos. Las siguientes opciones están disponibles:

- **Automático** - Bitdefender VPN seleccionará el protocolo óptimo para su dispositivo y red específicos.
- **Catapulta de hidra** - Rápido y seguro, ideal para streaming y juegos.
- **OpenVPN UDP** - Optimizado para velocidades rápidas. Sin embargo, este protocolo no es tan confiable en términos de pérdida de datos como otros protocolos de la lista.
- **OpenVPN TCP** - Diseñado para brindar confiabilidad. Garantiza que sus datos se entreguen en su totalidad, pero no es tan rápido como OpenVPN UDP.

- **guardacables** - Protocolo más nuevo, que proporciona una gran seguridad y un alto nivel de rendimiento.

doble salto

Con esta función puedes administrar los servidores a través de los cuales enviar y cifrar doblemente tu tráfico de Internet. Tus datos pasarán a través de dos servidores VPN en lugar de uno, lo que dificultará el seguimiento de tu actividad en Internet.

Nota
Solo puedes agregar un total de 5 ubicaciones de doble salto. Sin embargo, puede eliminar los saltos dobles personalizados de su lista y crear otros en cualquier momento.

Importante
El uso de servidores ubicados en diferentes continentes en el mismo doble salto puede ralentizar la velocidad de su conexión.

6. DESINSTALAR BITDEFENDER VPN

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

- **Desinstalar Bitdefender VPN de dispositivos Windows**
  - En **Windows 7**:
    1. Haga clic en **Inicio**, acceda al **Panel de control** y haga doble clic en **Programas y características**.
    2. Busque **Bitdefender VPN** y seleccione **Desinstalar**.
       Espere a que el proceso de desinstalación se complete.
  - En **Windows 8** y **Windows 8.1**:
    1. Desde la pantalla de inicio de Windows, localice el **Panel de control** (por ejemplo, puede empezar escribiendo "Panel de control" directamente en la pantalla Inicio) luego haga clic en su icono.
    2. Haga clic en **Desinstalar un programa** o **Programas y características**.
    3. Encontrar **Bitdefender VPN** y seleccione **Desinstalar**.
       Espere a que se complete el proceso de desinstalación.
  - En **Windows 10** y **Windows 11**:
    1. Haga clic en **Inicio** y, a continuación, haga clic en **Ajustes**.
    2. Haga clic en el icono del **Sistema** en el área de Configuración y, a continuación, seleccione **Aplicaciones instaladas**.
    3. Encontrar **Bitdefender VPN** y seleccione **Desinstalar**.
    4. Haga clic en **Desinstalar** para confirmar su elección.
       Espere a que se complete el proceso de desinstalación.
- **Desinstalar de dispositivos macOS**
  1. Haga clic en **Ir** en la barra de menús y seleccione **Aplicaciones**.
  2. Haga doble clic en la carpeta **Bitdefender**.
  3. Ejecute **BitdefenderUninstaller**.

4. En la nueva ventana, marque la casilla de verificación junto a **Bitdefender VPN** y, a continuación, haga clic en **Desinstalar**.
5. Escriba un nombre de cuenta de administrador y una contraseña válidos y luego haga clic en **OK**.
6. Por último, se le notificará que Bitdefender VPN se ha desinstalado correctamente. Haga clic en **Cerrar**.

- **Desinstalar de dispositivos Android**
  1. Abra la app de **Play Store**.
  2. Busque **Bitdefender VPN**.
  3. En la página de la tienda de aplicaciones Bitdefender VPN, seleccione **Desinstalar**.
  4. Confirme tocando en **OK**.
- **Desinstalar de dispositivos iOS**
  1. Toque y mantenga pulsado el icono de la app de Bitdefender VPN.
  2. Seleccione **Eliminar app**.
  3. Toque **Eliminar**.

7. PREGUNTAS FRECUENTES

¿Cuándo debo usar Bitdefender VPN?

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

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

¿Puedo elegir una ciudad con Bitdefender VPN?

Sí. Ahora, Bitdefender VPN para Windows, macOS, iOS y Android permite seleccionar una ciudad concreta. Esta es la lista de ciudades disponibles actualmente:

- **EE. UU.:** Atlanta, Charlotte, Chicago, Dallas, Denver, Houston, Los Ángeles, Miami, Nueva York, Newark, Phoenix, Portland, San José, Seattle y Washington
- **Canadá:** Montreal, Toronto y Vancouver
- **Reino Unido:** Londres y Mánchester

¿Se puede instalar Bitdefender VPN como app independiente?

La app de VPN se instala automáticamente junto con su solución de seguridad de Bitdefender. También puede instalarse como una app independiente desde la página del producto en Google Play Store y App Store.

¿Compartirá Bitdefender mi dirección IP y mis datos personales con terceros?

No, con Bitdefender VPN su privacidad está garantizada al 100 %. Nadie (agencias de publicidad, proveedores de Internet, empresas de seguros, etc.) tendrá acceso a sus registros online.

¿Qué algoritmo de cifrado utiliza?

Bitdefender VPN utiliza el protocolo Hydra en todas las plataformas, cifrado AES de 256 bits o el mayor cifrado disponible que sea compatible tanto con el cliente como con el servidor, con sistema de secreto perfecto hacia delante. Esto significa que se generan claves de cifrado para cada nueva sesión de VPN y se borran de la memoria al finalizarla.

¿Puedo acceder a contenidos restringidos geográficamente?

Con Premium VPN tiene acceso a una amplia red de ubicaciones virtuales de todo el mundo.

¿Disminuirá la duración de la batería de mi dispositivo?

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

¿Por qué ralentiza la VPN mi conexión a Internet?

Bitdefender VPN se ha diseñado para ofrecer una rápida navegación por la web. Dependiendo de la distancia entre su ubicación real y la del servidor al que elija conectarse, cabe esperar cierta disminución de la velocidad, pero casi siempre es tan poca que pasa desapercibida durante una actividad online normal. Además, disponemos de una de las infraestructuras de VPN más rápidas del mundo. Si no es imprescindible que se conecte desde su ubicación a un servidor lejano (por ejemplo, desde España hasta Estados Unidos), le recomendamos que permita que la VPN se conecte automáticamente al servidor más cercano o que encuentre un servidor más próximo a su ubicación actual.

8. OBTENIENDO AYUDA

8.1. Solicitando Ayuda

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

8.2. Recursos Online

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

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

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

8.2.1. Centro de soporte de Bitdefender

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

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

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

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

8.2.2. La comunidad de expertos de Bitdefender

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

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

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

https://community.bitdefender.com/es/

8.2.3. Ciberpedia de Bitdefender

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

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

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

8.3. Información de contacto

La comunicación eficiente es la clave para un negocio exitoso. Desde 2001, BITDEFENDER ha establecido una reputación incuestionable al esforzarse constantemente por mejorar la comunicación para superar las expectativas de nuestros clientes y socios. Si tiene alguna pregunta, no dude en contactarnos directamente a través de nuestro Centro de soporte de Bitdefender (página 31).

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

8.3.1. Distribuidores locales

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

Para encontrar un distribuidor de Bitdefender en su país:

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

GLOSARIO

Código de activación

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

ActiveX

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

Amenaza Persistente Avanzada

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

publicidad

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

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

Archivo

Disco, cinta o directorio conteniendo ficheros almacenados.

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

Puerta trasera

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

Sector de arranque

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

virus de arranque

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

red de bots

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

Navegador

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

Ataque de fuerza bruta

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

Línea de comando

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

Galletas

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

Ciberacoso

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

Ataque de diccionario

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

Disco duro

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

Descargar

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

Correo electrónico

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

Eventos

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

hazañas

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

Falso positivo

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

Extensión de nombre de archivo

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

Heurístico

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

Tarro de miel

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

IP

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

Subprograma de Java

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

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

registrador de teclas

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

Virus de macros

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

cliente de correo

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

Memoria

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

no heurístico

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

Depredadores en línea

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

Programas empaquetados

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

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

Camino

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

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

Suplantación de identidad

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

Fotón

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

Virus polimórfico

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

Puerto

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

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

Ransomware

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

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

Archivo de informe

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

Rootkit

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

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

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

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

Script

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

Spam

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

Spyware

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

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

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

Elementos de inicio

Todos los ficheros de esta carpeta se abren al iniciar el ordenador. Por ejemplo, una pantalla de inicio, un archivo de sonido para que se reproduzca cuando se inicie el equipo, un calendario de recordatorios o apps pueden ser elementos de inicio. Normalmente, se elige un alias del fichero para ubicar en esta carpeta y no directamente el fichero.

Suscripción

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

Bandeja del sistema

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

TCP/IP

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

Amenaza

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

Actualización de información sobre amenazas

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

Troyano

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

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

Actualizar

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

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

Red privada virtual (VPN)

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

Gusano

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