GUÍA DE USUARIO

Bitdefender CONSUMER SOLUTIONS

SecurePass

Bitdefender SecurePass

Guía de usuario

Publication date 20/11/2024
Copyright © 2024 Bitdefender

Aviso Legal

Reservados todos los derechos. Ninguna parte de este libro se puede reproducir ni transmitir de ninguna forma ni por ningún medio, electrónico o mecánico, incluidas las fotocopias, las grabaciones o cualquier sistema de recuperación y almacenamiento de información, sin el permiso por escrito de un representante autorizado de Bitdefender. La inclusión de citas breves en las reseñas solo puede ser posible con la mención de la fuente citada. El contenido no puede ser modificado de ninguna manera.

Advertencia y descargo de responsabilidad. Este producto y su documentación están protegidos por derechos de autor. La información en este documento se proporciona "tal cual", sin garantía. Aunque se han tomado todas las precauciones en la preparación de este documento, los autores no tendrán ninguna responsabilidad ante ninguna persona o entidad con respecto a cualquier pérdida o daño causado o presuntamente causado directa o indirectamente por la información contenida en este trabajo.

Este libro contiene enlaces a sitios web de terceros que no están bajo el control de Bitdefender, por lo que Bitdefender no es responsable del contenido de ningún sitio enlazado. Si accede a un sitio web de terceros enumerado en este documento, lo hará bajo su propio riesgo. Bitdefender proporciona estos enlaces solo para su comodidad, y la inclusión del enlace no implica que Bitdefender respalde o acepte ninguna responsabilidad por el contenido del sitio de terceros.

Marcas registradas. Los nombres de marcas registradas pueden aparecer en este libro. Todas las marcas comerciales registradas y no registradas en este documento son propiedad exclusiva de sus respectivos dueños y se reconocen respetuosamente.

Bitdefender

Tabla de contenidos

ACERCA DE ESTA GUÍA

Propósito y público al que se dirige

Esta guía va destinada a cualquier usuario de Bitdefender en todos los sistemas operativos compatibles (Windows, MacOS, iOS y Android) que haya elegido Bitdefender SecurePass como herramienta de gestión de contraseñas. La información presentada en ella no solo es adecuada para quienes posean conocimientos sobre informática, sino que es una guía accesible y sencilla para cualquiera.

Esta guía le ayudará a sacar el máximo partido a nuestro gestor de contraseñas superseguro y repleto en funciones y en ella se abordan detalladamente sus características y funcionalidades.

Le deseamos una lectura útil y agradable.

Cómo usar esta guía

Esta guía está organizada en diversos temas principales:

Primeros pasos (página 5)

Comencemos por Bitdefender SecurePass y su proceso de instalación.

Importación y exportación de sus contraseñas (página 10)

Comprenda cómo puede importar o exportar contraseñas dentro y fuera de SecurePass.

Características y funcionalidades (página 14)

Aprenda a usar Bitdefender SecurePass y todas sus características.

Obteniendo ayuda (página 27)

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 SECUREPASS

Bitdefender SecurePass es un servicio multiplataforma pensado para que los usuarios almacenen y organicen sus contraseñas online. Incorpora los algoritmos criptográficos más sólidos que se conocen, con el fin de ofrecer el más alto nivel de seguridad y protección digital. Funciona como una extensión del navegador y una solución de aplicación móvil para la administración de contraseñas e identidades, operaciones bancarias y demás información confidencial en todos los dispositivos.

Bitdefender SecurePass puede, automáticamente, almacenar, rellenar, generar y gestionar sus contraseñas para todos los sitios web y servicios online con la ayuda de una sola contraseña maestra, lo que facilita sobremanera la gestión de su identidad digital.

1.1. Versiones de evaluación y de pago de Password Manager

La versión de evaluación de Bitdefender Password Manager funciona en todos sus aspectos igual que la versión de pago del producto, pero su disponibilidad se limita a noventa días a partir de su activación.

> **Nota**
> Tenga presente que la versión de pago del producto puede adquirirse de forma totalmente independiente, pero las suscripciones a Bitdefender Premium Security y Bitdefender Ultimate Security incluyen el acceso ilimitado a Password Manager.

2. PRIMEROS PASOS

2.1. Requisitos del sistema

Puede utilizar la última versión de Bitdefender SecurePass únicamente en dispositivos con los siguientes sistemas operativos:

- **Para usuarios de PC:**
  - Windows 7 con Service Pack 1
  - Windows 8.1
  - Windows 10
  - Windows 11
- **Para usuarios de macOS:**
  - macOS 10.14 (Mojave) y sistemas operativos macOS posteriores

  Nota
  Tenga en cuenta que el rendimiento del sistema puede verse afectado en dispositivos que tengan CPU de generaciones anteriores.
- **Para usuarios de iOS:**
  - iOS 11.0 o sistemas operativos iOS posteriores
- **Para usuarios de Android:**
  - Android 5.1 y sistemas operativos Android posteriores

  Nota
  - La característica de desbloqueo por huella dactilar es compatible con **Android 6.0** y versiones posteriores.
  - La característica de autorrellenar es compatible con **Android 8.0** y versiones posteriores, así como con iPhone, iPad y iPod touch.

2.1.1. Requisitos de Software

Para poder usar Bitdefender SecurePass y todas sus características, los dispositivos Windows o macOS han de cumplir los siguientes requisitos de software:

- **Microsoft Edge** (basado en Chromium 80 y versiones posteriores)
- **Mozilla Firefox** (versión 65 o posterior)
- **Google Chrome** (versión 72 o posterior)
- **Safari** (versión 12 o posterior)

> **Nota**
> Los requisitos de software no se aplican a iOS y Android.

> **Advertencia**
> Si se incumplen los requisitos del sistema indicados anteriormente, no será posible instalar Bitdefender SecurePass o bien el producto no funcionará adecuadamente.

2.2. Pasos de la Instalación

Este capítulo le mostrará cómo instalar Bitdefender SecurePass tanto en los navegadores de su PC con Windows y macOS como en sus dispositivos móviles con Android o iOS.

> **Importante**
> Antes de proceder a la instalación, asegúrese de disponer de una suscripción válida a Password Manager en su cuenta de **Bitdefender Central** para que la extensión del navegador pueda comprobar la validez en su cuenta.
>
> Las suscripciones activas se muestran en la sección **Mis suscripciones** de Bitdefender Central.

2.2.1. Instalación en dispositivos Windows y macOS

A diferencia de la mayoría de las aplicaciones y software de escritorio que necesitan instalarse y configurarse en estos dispositivos, Bitdefender Password Manager se proporciona como extensión del navegador (lo que también se conoce como complemento) y puede añadirlo y habilitarlo rápidamente en el navegador que prefiera.

Los navegadores compatibles actualmente con el producto son los siguientes: **Google Chrome**, **Mozilla Firefox**, **Microsoft Edge** y **Safari**.

- **Google Chrome**
- **Mozilla Firefox**

- **Microsoft Edge**
- **Safari**

Para instalar Bitdefender SecurePass:

1. Tras comprar Bitdefender SecurePass, siga los pasos indicados en el correo electrónico de confirmación para activar la suscripción.
2. Inicie sesión en Bitdefender Central con sus credenciales.
   En el menú de la izquierda, selecciona **SecurePass**.
3. En el panel SecurePass, selecciona tu navegador preferido.
4. Instale la extensión del navegador:
   - **Google Chrome:**
     a. Haga clic en el **Añadir a Chrome** botón.
     b. En el cuadro de confirmación, haz clic **Añadir extensión**.
   - **Mozilla Firefox:**
     a. Haga clic en el **Añadir a Firefox** botón.
     b. Haga clic en el **Instalar** botón en la esquina superior derecha de la pantalla.
   - **Microsoft Edge:**
     a. Haga clic en el **Obtener** botón.
     b. Haga clic **Agregar extensión** en el mensaje que aparece.
   - **Safari:**
     a. El instalador de SecurePass se descargará en tu dispositivo macOS. Haz doble clic en el archivo descargado y sigue las instrucciones que aparecen en pantalla desde allí
     b. Al final del proceso de instalación, abra el **Safari** navegador y selección **Preferencias** en la barra de menú superior.
     c. En la ventana de Preferencias, haga clic en **Pestaña Extensiones**.
     d. Marca la casilla situada junto a **Bitdefender SecurePass** para habilitarlo.

Una vez instalada la extensión, puede continuar con Proceso de configuración (página 9).

2.2.2. Instalación en dispositivos Android

El método más sencillo para instalar Bitdefender Password Manager en teléfonos y tablets Android es descargar la aplicación directamente desde Google Play.

1. Antes que nada, después de la compra, asegúrese de abrir el correo electrónico de confirmación que recibió para seguir las instrucciones que se proporcionan allí para activar su suscripción a SecurePass.
2. Abre Google Play Store en tu dispositivo Android.
3. En la barra de búsqueda de Google Play Store, escribe **Bitdefender SecurePass**, localice y descargue la aplicación.
4. Una vez finalizada la descarga, abre la aplicación y, si es necesario, sigue los pasos de configuración que aparecen en pantalla para finalizar el proceso de instalación.

Con esto, ya ha finalizado la instalación en su dispositivo Android.

2.2.3. Instalación en dispositivos iOS

El método más sencillo para instalar Bitdefender Password Manager en dispositivos iOS y iPadOS es descargar la aplicación desde la App Store de Apple.

1. Antes que nada, después de la compra, asegúrese de abrir el correo electrónico de confirmación que recibió para seguir las instrucciones que se proporcionan allí para activar su suscripción a SecurePass.
2. Abre la App Store en tu dispositivo iOS.
3. En la barra de búsqueda de la App Store, escribe **Bitdefender SecurePass**, localice y descargue la aplicación.
4. Una vez finalizada la descarga, abre la aplicación y, si es necesario, sigue los pasos de configuración que aparecen en pantalla para finalizar el proceso de instalación.

Con esto, ya ha finalizado la instalación en su dispositivo iOS o iPadOS.

2.3. Proceso de configuración

Para configurar Bitdefender SecurePass en su navegador/dispositivo móvil:

1. Tras finalizar el proceso de instalación, abra la aplicación/extensión SecurePass e inicie sesión.
   Utilice las credenciales de la cuenta de Bitdefender asociada a su suscripción a SecurePass.
2. Se le pedirá que cree un **Contraseña maestra**.

   > **Importante**
   > Tenga en cuenta que necesitará esta contraseña maestra para desbloquear todas las contraseñas, información de tarjetas de crédito y notas guardadas en Bitdefender SecurePass. Básicamente, esta es la clave que permite al propietario utilizar

   Asegúrese de introducir una contraseña maestra segura sin correr el riesgo de olvidarla fácilmente.
   Una vez que se haya decidido por una contraseña maestra segura y única, haga clic en **Guardar y continuar**.
3. A continuación, se le proporcionará un **Clave de recuperación**.

   > **Advertencia**
   > Al crear la contraseña maestra, recibirá un **Clave de recuperación de 24 dígitos**. Anota tu clave de recuperación en un lugar seguro y no la pierdas. Esta clave es la única forma de acceder a las contraseñas guardadas en Password Manager en caso de que **olvida la contraseña maestra** configurada previamente para su cuenta.
   >
   > - Guarda la clave de recuperación copiándola en el portapapeles o descargándola como archivo PDF.
   >   Puede pulsar **Cerrar** cuando haya terminado.
4. Una vez hecho esto, selecciona **Acceda a su bóveda** botón.

Una vez finalizado el proceso de configuración, puede empezar a utilizar Bitdefender SecurePass.

3. IMPORTACIÓN Y EXPORTACIÓN DE SUS CONTRASEÑAS

Bitdefender Password Manager se ha diseñado para facilitar eficientemente la comunicación y la transferencia de datos con fuentes externas, plataformas y herramientas de software. Por eso, es posible satisfacer con facilidad la frecuente necesidad de importar o exportar contraseñas hacia o desde Bitdefender Password Manager.

3.1. Compatibilidad

Bitdefender Password Manager puede transferir datos sin problemas desde la siguiente lista de aplicaciones:

- Gestor de contraseñas de Bitdefender
- Monedero Bitdefender
- Bitdefender SecurePass
- Pase más seguro
- 1Contraseña
- Kaspersky
- Dashlane
- Navegador Chrome
- Navegador Firefox
- Microsoft Edge
- Bitwarden
- Último pase
- KeePass
- RoboForm

Dicha transferencia de datos entre Bitdefender Password Manager y otro software de gestión de cuentas puede realizarse a través de los siguientes formatos de datos:

CSV, **JSON**, **XML**, **TXT**, **1pif** y **FSK**.

3.2. Importación a Password Manager

Bitdefender Password Manager le permite importar fácilmente contraseñas desde otros gestores de contraseñas y navegadores. Si está pensando en pasarse a Bitdefender Password Manager desde otro servicio de gestión de contraseñas, lo más probable es que ya tenga almacenadas una considerable cantidad de credenciales, como nombres de usuario, contraseñas y otros datos de inicio de sesión necesarios para todas sus cuentas.

Puesto que ha elegido Bitdefender Password Manager, deseará importar esos datos que tiene guardados.

A continuación se explica cómo importar a Bitdefender Password Manager la información almacenada en otras aplicaciones y navegadores, **independientemente del sistema operativo** en el que haya elegido instalar este producto:

1. Abra Bitdefender SecurePass y vaya a **Ajustes**.
   - En el navegador:
     Haga clic en **Ajustes** en la esquina superior derecha de la página.
   - En la aplicación:
     Toca el **Más** en la esquina inferior derecha de la pantalla y, en la parte superior de la lista que aparece a continuación, toca **Ajustes**.
2. En el **Copia de seguridad y restauración** sección, selecciona **Importar contraseñas**. Se abrirá la ventana de importación.
3. Seleccione el nombre del administrador de contraseñas o del navegador web que haya utilizado anteriormente en el menú desplegable al que se puede acceder a través de **Seleccione el tipo de archivo** campo.

   > **Nota**
   > Si se utilizó una contraseña para cifrar el archivo, se le pedirá que la introduzca en el **Contraseña** campo; de lo contrario, puede dejarlo en blanco.

4. Seleccione el **Seleccione el archivo que desea importar** archivado.

Navega hasta la ubicación en la que se guardaron los datos exportados que pertenecían a tu antiguo gestor de contraseñas. Elija el archivo una vez que lo encuentre y, a continuación, haga clic **Abrir**.

5. Tras seleccionar el archivo, seleccione **Importar** en la esquina inferior izquierda de la ventana de importación. El proceso comenzará en breve, acompañado de una barra de progreso

Una vez importadas, podrá acceder a sus contraseñas en todos los dispositivos en los que instale la aplicación Bitdefender Password Manager o la extensión del navegador.

> **Nota**
> Al volver a su bóveda de contraseñas en SecurePass, verá una carpeta llamada **Importar**, que contiene todos los datos de tu gestor de contraseñas o navegador web anterior.

3.3. Exportación desde Password Manager

Bitdefender Password Manager le permite exportar fácilmente las contraseñas que haya almacenado en él (incluso las credenciales de inicio de sesión de cuentas, notas seguras, etc.) a un archivo CSV (valores separados por comas) o un archivo cifrado, por si alguna vez desea pasarse a otro servicio gestor de contraseñas, para que su cambio desde Bitdefender Password Manager no le resulte difícil.

> **Importante**
> Los archivos CSV **no** están cifrados y contienen nombres de usuario y contraseñas en texto sin formato, por lo que cualquiera que tenga acceso a su dispositivo podría leer su información privada. Por lo tanto, le recomendamos que siga las instrucciones que se exponen a continuación en un dispositivo de confianza.

Puede exportar sus datos desde Bitdefender Password Manager de la siguiente manera:

1. Abra Bitdefender SecurePass y vaya a **Ajustes**.
   - En el navegador:
     Haga clic en **Ajustes** en la esquina superior derecha de la página.
   - En la aplicación:
     Toca el **Más** en la esquina inferior derecha de la pantalla y, en la parte superior de la lista que aparece a continuación, toca **Ajustes**.

2. En el **Copia de seguridad y restauración** sección, selecciona **Exportar contraseñas**. Se abrirá la ventana de exportación.
3. Haga clic en **Seleccione el tipo de archivo**. En el menú desplegable, elige exportar tus datos en formato JSON o CSV. También puedes introducir una contraseña para proteger el archivo exportado.
   Marca la casilla correspondiente si también quieres incluir elementos compartidos.
4. Haga clic **Exportar** en la esquina inferior izquierda de la ventana de exportación y guarda el archivo exportado en tu dispositivo.

4. CARACTERÍSTICAS Y FUNCIONALIDADES

Este capítulo abordará todas las características y funcionalidades de Bitdefender Password Manager, explicando su utilidad y cómo utilizarlas más eficientemente.

4.1. Guardar contraseñas manualmente

Puede almacenar de forma segura información como contraseñas, credenciales y otros datos, como información de tarjetas de crédito o notas en Bitdefender SecurePass de forma manual, de la siguiente manera:

1. Abra Bitdefender SecurePass
2. En el **Mi bóveda** pestaña, pulse la **+Añadir elemento** botón.
3. Selecciona el tipo de artículo que quieres añadir. (cuenta, tarjeta de crédito, identidad o nota).
4. Rellene los campos obligatorios en función del elemento seleccionado.
5. Tras completar todos los detalles necesarios, guarde el artículo para añadirlo a su bóveda de SecurePass.

4.2. Generador de contraseñas

Bitdefender SecurePass incluye una función de generación de contraseñas que puede ayudar a crear contraseñas seguras.

Para acceder y usar el generador de contraseñas:

1. Abra Bitdefender SecurePass y acceda a **Genere la contraseña** pestaña en el lado izquierdo de la pantalla. Esto lo llevará al generador de contraseñas integrado en SecurePass
2. Personalice la contraseña que va a generar de acuerdo con sus propias necesidades y preferencias.
   - Longitud de la contraseña: arrastre el control deslizante para determinar si tiene entre 8 y 32 caracteres.

- Letras mayúsculas y minúsculas: selecciona qué tipo de letras quieres añadir (o ambos) según el nivel de complejidad de tu contraseña.
- Números: Al marcar esta casilla, se incluirán números en la cadena de caracteres que compone la contraseña.
- Caracteres especiales: añada símbolos a la contraseña para aumentar la complejidad de la contraseña.

> **Nota**
> Pulsa el **Guardar la configuración** botón para que SecurePass las recuerde y genere siempre contraseñas en función de la configuración que haya guardado.

3. Genere una nueva contraseña haciendo clic en el icono de flecha circular situado debajo de la contraseña que se muestra actualmente. Cada clic genera una nueva cadena de caracteres.
4. Una vez que esté satisfecho con la contraseña generada, puede copiarla en el portapapeles o hacer clic en el **Guardar cuenta** botón para guardarla en tu bóveda (asociándola con otra información de la cuenta).

> **Nota**
> También puede generar rápidamente una contraseña **directamente desde los formularios de registro** haciendo clic en el icono de Bitdefender SecurePass que aparece en el campo de contraseña de la página de registro. Al hacer clic en él, puede elegir **Generar contraseña** opción.

4.3. Verificación de seguridad de la contraseña

Bitdefender SecurePass ofrece la posibilidad de evaluar la seguridad de las contraseñas y los datos confidenciales guardados. Se trata de una función vital a la hora de evaluar y valorar cualquier posible vulnerabilidad en relación con la privacidad y la seguridad de sus datos

Para comprobar la seguridad de las contraseñas almacenadas:

1. Abra Bitdefender SecurePass y, en el menú de correo, seleccione **Informe de seguridad** pestaña.

La pestaña Informe de seguridad se divide en cuatro secciones: infringida, débil, antigua y duplicada.

2. La cantidad de contraseñas que pertenecen a cada una de las cuatro categorías se mostrará en la pantalla.
   Además, al revisar la lista de contraseñas almacenadas, cada contraseña se etiquetará con la categoría en la que se encuentra.

Para entender el significado de estos niveles de seguridad, a continuación se presentan algunos detalles breves sobre cada uno de ellos:

- Contraseñas violadas: si alguna de sus credenciales ha sido parte de una violación de datos, aparecerá en la lista **infringido** sección.

  > **Nota**
  > Para comprobar si alguna de tus contraseñas se ha visto comprometida y se ha filtrado debido a violaciones de datos, haz clic en **Ejecute un análisis de seguridad** botón.

- Contraseñas débiles: SecurePass identificará y marcará **débil** las contraseñas almacenadas en su bóveda se basan en un algoritmo interno que se ejecuta localmente y que tiene en cuenta varios criterios, como la longitud de la contraseña, la variedad de caracteres y la inclusión de dígitos o letras mayúsculas, entre otros factores.
- Contraseñas antiguas: las contraseñas que se hayan guardado y no se hayan modificado durante un período superior a seis meses se marcarán como **antiguas**.
- Contraseñas duplicadas: teniendo en cuenta que el uso de las mismas contraseñas en varias plataformas y cuentas presenta un gran riesgo de seguridad, SecurePass marcará las contraseñas utilizadas en más de un lugar como **duplicado**.

4.4. Organización de datos

Dentro de Bitdefender SecurePass, puede organizar y, por lo tanto, administrar más fácilmente todos los elementos guardados.

Puedes clasificar tus elementos en carpetas específicas para acceder fácilmente a ellos siguiendo estos pasos:

1. Abra Bitdefender SecurePass y vaya a **Mi bóveda**. Aquí, toca el **Añadir carpeta** botón.

2. Ponle un nombre a la carpeta y toca el **Crea** botón.
   La nueva carpeta aparecerá ahora en tu bóveda.

Para mover elementos a la carpeta que has creado:

1. Haz clic en cualquier cuenta que quieras mover y pulsa el **Editar** botón.
2. Pulsa la ubicación que se muestra junto a **Guarda el artículo en** y seleccione el nombre de la carpeta en la lista desplegable.
3. Pulsa el **Guardar cuenta** botón.

La cuenta ahora se almacenará en la carpeta seleccionada.

4.5. Llenado automático inteligente

Bitdefender SecurePass le permite rellenar automáticamente las credenciales y la información de la cuenta en cualquier formulario de inicio de sesión en línea.

> **Nota**
> Como extensión de navegador web, en Windows o macOS, la función Autocompletar debería funcionar sin problemas.

4.5.1. Autocompletar en Android

Para configurar SecurePass en Android con el fin de usar la función de llenado automático:

1. Abra la aplicación Bitdefender SecurePass en su dispositivo Android.
2. Toca el **Más** botón de menú.
3. En la parte superior de la pantalla, toca **Ajustes**.
4. Pulsa **Convierte este en tu gestor de contraseñas predeterminado**
5. Activa Bitdefender SecurePass en la lista de servicios de autocompletar.

> **Nota**
> También puedes ir a la configuración de tu dispositivo Android, en **Contraseñas y cuentas** > **Servicio de llenado automático** > habilita Bitdefender SecurePass.
>
> Para Android 11 o versiones anteriores del sistema operativo, la configuración es la siguiente: **Sistema** > **Idioma y entrada** > **Avanzado**.

6. Grifo **OK**.

Una vez hecha esta configuración, cada vez que toques un campo de inicio de sesión, aparecerá en tu pantalla una opción llamada Bitdefender SecurePass. Puedes tocarla para abrir la aplicación. Inicie sesión en SecurePass y sus credenciales se rellenarán automáticamente

4.5.2. Autocompletar en iOS

Para configurar SecurePass en su dispositivo iOS para usar la función de llenado automático:

1. Abra el **Configuración** aplicación en tu iPhone o iPad, y selecciona **General**.
2. Pulsa **Relleno automático y contraseñas**. Garantiza la opción **Rellenar automáticamente contraseñas y claves de acceso** o **Rellenar contraseñas automáticamente** - según la versión de iOS - está activado.
3. En el **Formulario de llenado automático** lista, habilite el **Bitdefender SecurePass** aplicación.

Una vez hecha esta configuración, cada vez que toques un campo de inicio de sesión, aparecerá en tu pantalla una opción llamada Bitdefender SecurePass. Puedes tocarla para abrir la aplicación. Inicie sesión en SecurePass y sus credenciales se rellenarán automáticamente

4.5.3. Detalles de la tarjeta de llenado automático

Si bien SecurePass proporciona un icono de fácil acceso para rellenar automáticamente las credenciales de inicio de sesión y las contraseñas, la función de llenado automático de la información de las tarjetas de crédito funciona de forma diferente:

1. Navega hasta la página de pago o pago del sitio web en el que deseas utilizar la información de tu tarjeta de crédito almacenada.
2. Haga clic con el botón derecho en cualquier área en blanco de la página de pago. Esto hará que aparezca el menú contextual en la pantalla.
3. Selecciona Bitdefender SecurePass en el menú pasando el cursor sobre la opción. Se abrirá un submenú
4. Elige el **Rellenar automáticamente la información de la tarjeta de crédito**. Aparecerá una lista de las tarjetas de crédito que hayas guardado en la bóveda de SecurePass
5. Selecciona la tarjeta preferida.

De esta forma, SecurePass rellenará automáticamente los campos del formulario de pago con los detalles de la tarjeta de crédito que haya elegido.

5. ÚSELO COMO UNA APLICACIÓN DE 2FA

Siempre puedes optar por utilizar Bitdefender SecurePass como una aplicación de autenticación de dos factores para cualquier sitio web o plataforma que desees, y gestionar tus códigos de autenticación de dos factores junto con tus contraseñas de la siguiente manera:

1. Ve a la configuración de seguridad del sitio web o la aplicación en la que deseas habilitar la función 2FA. Normalmente, se te presentará un código QR o un código de verificación durante el proceso
2. Inicie Bitdefender SecurePass y acceda a la cuenta correspondiente que desea configurar para el uso de la 2FA. Haga clic en **Editar** botón.
3. Desplázate hasta la parte inferior de la página de ingreso de la cuenta en SecurePass y presiona el **Autenticación de dos factores** opción.
4. Escanea el código QR o introduce el código manualmente.
   Una vez hecho esto, SecurePass confirmará la correcta configuración de la autenticación de dos factores.
5. Después de esto, pulse el botón nuevo **Ver código** el botón ahora está visible en la interfaz. Allí se muestra un código urgente
6. Vuelve a la cuenta en la que habilitaste la función 2FA e introduce el código de Bitdefender SecurePass para verificar tu configuración.

Tras completar este proceso de configuración, pulse **Guardar cuenta** botón en SecurePass para finalizar el proceso.

A partir de ahora, cuando inicies sesión en la plataforma para la que hayas configurado la función 2FA, se te pedirá que utilices los códigos 2FA de SecurePass para la cuenta correspondiente, lo que ofrece un nuevo nivel de seguridad para la cuenta en cuestión.

6. COMPARTIR DATOS

Bitdefender SecurePass incluye la posibilidad de compartir información confidencial de forma segura, como credenciales, contraseñas o detalles de tarjetas de crédito.

Puedes usar la función de compartir a través de los siguientes enlaces:

1. Elige un objeto almacenado en tu bóveda.
   - En el navegador:
     Ve a tu bóveda y haz clic en el elemento que quieres compartir. En el lado derecho, haz clic en el menú de tres puntos y selecciona **Compartir enlace**.
   - En la aplicación:
     Ve a tu bóveda y toca el elemento que quieres compartir. Pulsa el icono del enlace y elige el **Generar enlace para compartir** opción.
2. Cree el enlace Compartir especificando:
   - La fecha de caducidad del enlace.
   - El límite de uso.
   - Si el enlace debe estar protegido con contraseña o no.
3. Una vez generado, copia el enlace generado y envíalo al destinatario previsto.

6.1. Compartir con grupos

Los grupos se crean con el fin de facilitar aún más el intercambio de datos. Puede crear varios grupos dentro de Bitdefender SecurePass con otros usuarios para compartir datos confidenciales de forma segura

1. Crea un grupo:
   - Ir a **Grupos** y pulse el **Crear grupo** botón dentro de la pestaña Grupos.
   - Establezca un nombre para el grupo y, a continuación, pulse la **Crea un grupo** botón.
2. Añadir elementos a los grupos:

- En el navegador:
  Ve a tu bóveda y haz clic en el elemento que quieres compartir. Haz clic en el menú de tres puntos situado a la derecha del elemento y elige **Añadir al grupo**.
- En la aplicación:
  Ve a tu bóveda y haz clic en el elemento que quieres compartir. Elige el **Compartir con el grupo** opción.

Selecciona el grupo con el que quieres compartir el elemento.

3. Establezca los derechos de acceso (lectura, escritura, concesión) en función del nivel de control que desee proporcionar a los miembros del grupo.
4. Prensa **Guardar**, entonces **Hecho**.

Tú y los miembros del grupo pueden revisar los elementos compartidos en la sección del grupo.

6.2. Administrar grupos

En el **Grupos** En la sección de Bitdefender SecurePass puedes revisar todos los grupos creados y administrarlos en función de tus necesidades:

- Cambie el nombre de los grupos.
- Editar miembros. (invitar a nuevos miembros, asignar derechos a miembros específicos, conceder derechos de administración o de uso compartido y eliminar a los miembros existentes)
- Abandona los grupos.
- Eliminar grupos.

7. BLOQUEAR CUENTA

Bitdefender SecurePass viene con un **Bloquear cuenta** función que bloquea instantáneamente su cuenta y termina todas las sesiones activas en todos los dispositivos que tienen acceso a ella. Esta función es especialmente útil cuando surgen sospechas de acceso no autorizado

Para bloquear su cuenta de SecurePass:

1. Abra Bitdefender SecurePass.
2. Una vez en SecurePass:
   - En el navegador:
     Haga clic en **Ajustes** en la esquina superior derecha de la página.
   - En la aplicación móvil:
     Toca el **¡Protégeme** botón de menú.
3. Pulsa el **Bloquear cuenta** botón para cerrar sesión instantáneamente en todos los dispositivos y terminar las sesiones en curso.

8. PREGUNTAS FRECUENTES

Hay ciertas preguntas sobre Bitdefender Password Manager que suelen plantearse con frecuencia. ¡Tenemos las respuestas! Aquí puede obtener más información sobre su cuenta de Bitdefender, la importación de las contraseñas, los protocolos de seguridad de datos y otros temas importantes para nuestros clientes.

Preguntas generales acerca de Bitdefender Password Manager

¿Qué sucede cuando expira Bitdefender Password Manager?

Cuando expire su suscripción a Password Manager y deje de estar activa, dispondrá de un máximo de noventa días para exportar sus contraseñas, de las cuales se conservará copia de seguridad durante otros treinta días más. Durante esos noventa días, solo podrá exportar sus datos; no podrá seguir usando Password Manager. La características autorrellenar dejará de funcionar, al igual que la generación de contraseñas.

Finalizado el período de gracia de noventa días, cuenta con treinta días más para ponerse en contacto con el servicio de soporte técnico de Bitdefender y solicitar restaurar sus contraseñas a la base de datos activa. Entonces, podrá exportar sus contraseñas desde Bitdefender Password Manager.

Sus datos se mantendrán en la base de datos activa solo hasta finalizar el día en que se solicitó su restauración. A medianoche se borrará la base de datos y, si aún no ha sobrepasado el período adicional de treinta días, las contraseñas podrán restaurarse nuevamente desde la copia de seguridad. Los datos sin procesar de la base de datos de la copia de seguridad pueden proporcionarse al usuario si lo solicita, pero la base de datos está cifrada y no es posible acceder a la información.

¿Qué es una contraseña maestra y por qué tengo que recordarla?

La contraseña maestra es la puerta de acceso a todas las contraseñas almacenadas en su cuenta de Bitdefender Password Manager. La contraseña maestra debe tener al menos ocho caracteres. Así pues, cree una contraseña maestra segura, memorícela y no se la revele nunca a nadie. Para crear una contraseña maestra segura, le recomendamos que

utilice una combinación de letras mayúsculas y minúsculas, números y caracteres especiales (como por ejemplo #, $ o @).

¿Por qué no guardan mi contraseña maestra y qué sucede si la olvido?

No almacenamos su contraseña maestra en nuestros servidores para que solo usted pueda acceder a su cuenta. Es lo que más seguridad aporta. Si Bitdefender Password Manager no reconoce su contraseña maestra, asegúrese de haberla escrito correctamente y de que no esté activada la tecla de Bloq Mayús en su teclado.

Si olvida su contraseña maestra, siempre puede recurrir a la clave de recuperación para desbloquear Password Manager. Durante el proceso de registro, Bitdefender Password Manager le proporciona una {1}clave de recuperación{2} que puede utilizar para recuperar el acceso a su cuenta sin perder los datos.

¿Qué es el modo offline?

El modo sin conexión se activa automáticamente cuando se interrumpe la conexión a Internet mientras se utiliza Bitdefender SecurePass. Si ya ha iniciado sesión y ha introducido su contraseña maestra, el modo sin conexión le permite acceder a sus contraseñas cuando la conexión a Internet está fuera

¿Cómo desinstalo Bitdefender Password Manager?

Para desinstalar Bitdefender Password Manager:

- En Windows y macOS:
  Elimine la extensión de Password Manager de su navegador. Haga clic con el botón derecho en el icono de Bitdefender y seleccione “Eliminar”.
- Para Android:
  Toque y mantenga pulsado el icono de la aplicación Password Manager y, a continuación, arrástrelo a la parte superior de la pantalla, donde dice “Desinstalar”.
- En iOS y iPadOS:
  Toque y mantenga pulsado el icono de la aplicación Password Manager hasta que todas las aplicaciones de su pantalla empiecen a moverse y, a continuación, toque la X en la parte superior izquierda del icono de Bitdefender.

Preguntas sobre privacidad y seguridad acerca de Bitdefender Password Manager

¿Pueden ver mis contraseñas los empleados de Bitdefender?

En absoluto. Su privacidad es nuestra principal prioridad. Esta es la razón principal por la que no almacenamos su contraseña maestra en nuestros servidores de datos: para que nadie pueda acceder a su cuenta, ni siquiera los empleados de la empresa. Las contraseñas y las cuentas están altamente cifradas con el algoritmo de seguridad de datos más sólido y el código que vemos parece simplemente una cadena aleatoria de números y letras sin sentido.

¿Qué pasaría si pirateasen los servidores de Password Manager?

Las contraseñas se cifran localmente en su dispositivo antes de que lleguen a nuestros servidores, de modo que si los piratas informáticos lograsen penetrar en nuestro sistema, al carecer de su clave para descifrarlas, solo obtendrían páginas de letras y números aleatorios. Esto significa que usted y los datos de su cuenta están siempre a salvo con nosotros.

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 27).

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 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.