GUÍA DE USUARIO

Bitdefender CONSUMER SOLUTIONS

Password Manager

Bitdefender Password Manager

Guía de usuario

Fecha de publicación 06/09/2023

Aviso Legal

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 Password Manager 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 Password Manager y su proceso de instalación.

Características y funcionalidades (página 20)

Aprenda a usar Bitdefender Password Manager y todas sus características.

Obteniendo ayuda (página 32)

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 PASSWORD MANAGER

Bitdefender Password Manager 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 Password Manager 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. Seguridad y cómo funciona

El software Bitdefender Password Manager se basa en algunos de los últimos algoritmos criptográficos que garantizan la mayor seguridad de datos que un usuario pueda esperar, como los protocolos AES-256-CCM, SH512, BCRYPT, HTTPS y WSS para la transmisión de datos. Todos los datos tratados se hayan cifrados en todo momento y se descifran localmente. Así, nadie más que el titular puede acceder a la información almacenada en su cuenta, así como conocer la contraseña maestra que se emplea para acceder y, posteriormente, hacer uso de los datos.

1.2. 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 Password Manager únicamente en dispositivos con los siguientes sistemas operativos:

- **Para usuarios de PC:**
  - Windows 7 con Service Pack 1
  - Windows 8
  - 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 Password Manager 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 Password Manager o bien el producto no funcionará adecuadamente.

2.2. Pasos de la Instalación

Este capítulo le mostrará cómo instalar Bitdefender Password Manager 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**.

1. Acceda a https://central.bitdefender.com/ e inicie sesión en su cuenta. Si aún carece de ella, haga clic en **CREAR CUENTA** y, a continuación, escriba su nombre completo, una dirección de correo electrónico y una contraseña.
2. Seleccione **Mis dispositivos** en la barra lateral izquierda de la pantalla.
3. En la sección **Mis dispositivos**, haga clic en **+ Añadir dispositivo**.
4. Esto hará que aparezca una nueva ventana. En la pantalla de selección, elija **Password Manager**.
5. Elija **Este dispositivo**.
   Si desea instalarlo en un dispositivo diferente, seleccione Otros dispositivos. A continuación, puede enviar por correo electrónico un enlace de descarga al dispositivo que desee o copiar directamente la URL para proceder a la instalación.
6. Lo siguiente es elegir en qué navegador desea instalar la extensión Password Manager.
7. Los respectivos botones le redirigirán a la tienda de extensiones del navegador. A partir de ahí, limítese a seguir las instrucciones que aparecen en la pantalla, como se indica a continuación:

   Microsoft Edge

   - Haga clic en el botón **Obtener**
   - Haga clic en **Agregar extensión** en el mensaje que aparece en la pantalla

   Google Chrome

   - Haga clic en el botón **Añadir a Chrome**
   - En el cuadro de confirmación, haga clic en **Añadir extensión**

   Mozilla Firefox

   - Haga clic en el botón **Agregar a Firefox**
   - En el cuadro de confirmación, haga clic en **Añadir**

   Safari

- Haga clic en el botón **Obtener** y, luego, en **Instalar**
- Abra Safari y seleccione **Preferencias** en la barra de menú superior
- En la ventana de Preferencias, haga clic en la pestaña **Extensiones**
- Marque la casilla de verificación junto a Password Manager para habilitarlo

Tras haber seguido estos pasos, establezca una contraseña maestra segura y, a continuación, pulse el botón **Guardar contraseña maestra** después de haber leído y aceptado los **Términos y condiciones**.

Importante

Tenga en cuenta que necesitará esta contraseña maestra para desbloquear todas las contraseñas, la información de su tarjeta de crédito y las notas guardadas en Bitdefender Password Manager. Esta es, básicamente, la clave que permite al propietario utilizar el producto.

Advertencia

Tras crear su contraseña maestra, recibirá una **clave de recuperación de 24 dígitos**. **Anótela en un lugar seguro y no la pierda**. Esta clave será la única manera de acceder a sus contraseñas guardadas en Password Manager en caso de que {5}olvidase la contraseña maestra{6} establecida para su cuenta en el paso anterior.

- Puede pulsar **Cerrar** cuando haya terminado.

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.

También puede instalar la aplicación Bitdefender Password Manager desde su cuenta de **Bitdefender Central**:

1. En su dispositivo móvil Android, inicie sesión en su cuenta de Bitdefender Central accediendo a https://login.bitdefender.com/central/login.

2. Seleccionar **Mis dispositivos** en la barra lateral izquierda de la pantalla.
3. En el **Mis dispositivos** sección, proceda haciendo clic en **+ Agregar dispositivo**.
4. Esta acción hará que aparezca una nueva ventana. Elegir **Administrador de contraseñas** en la pantalla de selección.
5. Elegir **Este dispositivo**.
   Si desea instalarlo en un dispositivo diferente, seleccione **Otros dispositivos**. A continuación, puede enviar por correo electrónico un enlace de descarga al dispositivo que desee o copiar directamente la URL para proceder a la instalación.
6. Se le redirigirá a **Google Play**. Toque **Instalar** para descargar Bitdefender Password Manager en Android.
7. Una vez finalizada la descarga, abra la aplicación Password Manager.
8. Si no se inicia sesión en su cuenta automáticamente, hágalo con su nombre de usuario y contraseña.
   Una vez que haya seguido estos pasos, establezca una contraseña maestra segura, luego presione el botón **Guardar contraseña maestra** después de leer y estar de acuerdo con el **Términos y condiciones**.

> **Importante**
> Tenga en cuenta que necesitará esta contraseña maestra para desbloquear todas las contraseñas, la información de la tarjeta de crédito y las notas guardadas en Bitdefender Password Manager. Esta es esencialmente la clave que permite al propietario utilizar este producto.

Advertencia

Al crear la contraseña maestra, recibirá una **clave de recuperación de 24 dígitos**. Tome nota de su clave de recuperación en un lugar seguro y no la pierda. Esta clave es la única forma de acceder a sus contraseñas guardadas en el Administrador de contraseñas en caso de que **olvida la contraseña maestra** configurado previamente para su cuenta.

- Puedes presionar **Cerca** cuando termine.

9. Cree un **PIN de cuatro dígitos** para que si se pasa a otra aplicación y luego regresa a Password Manager no tenga que volver a introducir la contraseña maestra que estableció anteriormente. En caso de estar disponible, también puede habilitar el reconocimiento facial o la autenticación por huella dactilar.
10. Toque en **Activar autocompletar** para configurar los ajustes de autocompletar de Android.

Nota

Si omite este paso, puede habilitar y personalizar más adelante las características de autocompletar de Android siguiendo las instrucciones indicadas en Autorrellenado inteligente (página 21).

11. Se encontrará con una lista de aplicaciones en las que se pueden autocompletar las contraseñas.
    Seleccione **Password Manager** y, luego, el dispositivo le solicitará que confirme su confianza en esta aplicación.
    Toque en **Aceptar**.
12. Introduzca el PIN que estableció en el **paso 9** para confirmar esta acción.

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.

Download on the App Store

La instalación de la aplicación Bitdefender Password Manager también se puede realizar a través de su Centro de Bitdefender cuenta:

1. En su iPhone o iPad, inicie sesión en su cuenta de Bitdefender Central accediendo a https://login.bitdefender.com/central/login.
2. Seleccionar **Mis dispositivos** en la barra lateral izquierda de la pantalla.
3. En el **Mis dispositivos** sección, proceda haciendo clic en **+ Agregar dispositivo**.
4. Esta acción hará que aparezca una nueva ventana. Elegir **Administrador de contraseñas** en la pantalla de selección.
5. Elegir **Este dispositivo**.
   Si desea instalar en un dispositivo diferente, seleccione **Otros dispositivos**. A continuación, puede enviar por correo electrónico un enlace de descarga al dispositivo respectivo o copiar directamente la URL para la instalación.
6. Se le redirigirá a la **App Store**. Toque en el icono de la nube con una flecha apuntando hacia abajo para descargar Bitdefender Password Manager para iOS.
7. Una vez instalada la aplicación , ábrala y marque la casillita de la pantalla. Tras leer y aceptar el **Acuerdo de suscripción**, seleccione **Continuar**.
8. Si no inicia sesión automáticamente en su cuenta, inicie sesión con su nombre de usuario y contraseña.
   Una vez que haya seguido estos pasos, establezca una contraseña maestra segura, luego presione el botón **Guardar contraseña maestra** después de leer y estar de acuerdo con el **Términos y condiciones**.

> **Importante**
> Tenga en cuenta que necesitará esta contraseña maestra para desbloquear todas las contraseñas, la información de la tarjeta de crédito y las notas guardadas en Bitdefender Password Manager. Esta es esencialmente la clave que permite al propietario utilizar este producto.

Advertencia

Al crear la contraseña maestra, recibirá una **clave de recuperación de 24 dígitos**. Tome nota de su clave de recuperación en un lugar seguro y no la pierda. Esta clave es la única forma de acceder a sus contraseñas guardadas en el Administrador de contraseñas en caso de que **olvida la contraseña maestra** configurado previamente para su cuenta.

- Puedes presionar **Cerca** cuando termine.

9. Crear un **PIN de 4 dígitos**, por lo que si cambia a otra aplicación y luego regresa al Administrador de contraseñas, no tendrá que volver a ingresar la contraseña maestra que configuró anteriormente. Si está disponible, también puede habilitar el reconocimiento facial o la autenticación de huellas dactilares.

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

3. PLAN COMPARTIDO

Bitdefender Password Manager Shared Plan permite a múltiples usuarios acceder y utilizar la misma suscripción. Proporciona un enfoque centralizado para el acceso al software, administración y soporte, ofreciendo una solución rentable para compartir el servicio de gestor de contraseñas entre múltiples usuarios.

- El responsable del plan de suscripción compartido, conocido como Plan Manager, puede compartir el servicio entre los miembros.
- Cada miembro obtiene su propia y única cuenta Bitdefender Central vinculada a su dirección de correo electrónico y acceso al servicio Password Manager.

3.1. Compartir Bitdefender Password Manager con múltiples usuarios

Invitar miembros

Para agregar uno o varios usuarios a la suscripción compartida, el administrador del plan debe seguir estos pasos:

1. Inicie sesión en su cuenta de Bitdefender Central en https://central.bitdefender.com/
2. Vaya al menú **Mis suscripciones** situado en la parte izquierda de la página.
3. Seleccione **Invitar miembro** en el panel **Bitdefender Password Manager Shared Plan**.
4. Introduzca el email de cada persona con la que desea compartir su suscripción y haga clic en **Enviar**. Se pueden añadir un máximo de 3 miembros a la vez.
5. Las instrucciones de configuración se enviarán inmediatamente por correo electrónico a los nuevos miembros. Haga clic en **Cerrar** para salir de la ventana de confirmación.

Nota

Los miembros tienen 24 horas para aceptar su invitación una vez que se les envía por correo electrónico.

- Los miembros invitados aparecerán con el estado "Invitado".
- Los verás como miembros "activos" después de que acepten la invitación. También se le notifica por correo electrónico de cada invitación aceptada.

Eliminar miembros

El acceso al plan compartido de Bitdefender Password Manager se pierde para los miembros que son eliminados. Cuando el administrador del plan decide eliminar un miembro de la suscripción, el miembro recibe una notificación por correo electrónico. Durante los siguientes 30 días, el ex-miembro es cambiado a una versión de prueba de 30 días de Bitdefender Password Manager con todas las capacidades. A continuación, el servicio se desactivará.

El administrador del plan puede excluir usuarios del plan compartido de la siguiente forma:

1. Inicie sesión en su cuenta de Bitdefender Central en https://central.bitdefender.com/
2. Vaya al menú **Mis suscripciones** situado en la parte izquierda de la página.
3. En el panel **Bitdefender Password Manager Shared Plan**, haga clic en **Administrar** y, a continuación, seleccione **Editar miembros** en el menú.
4. Haga clic en el botón **Eliminar** para sacar a un miembro del plan compartido.
5. Seleccione **Sí, eliminar miembro** y haga clic en el botón **Finalizar edición** para que los cambios surtan efecto.

Nota

Cuando se elimina un miembro del plan compartido, su estado cambia a **Pendiente de eliminación** hasta que se elimine por completo

Aceptar una invitación

Recibirá un correo electrónico cuando alguien le invite a convertirse en miembro de suscripción del plan compartido de Bitdefender Password Manager. Tienes 24 horas para aceptar una invitación una vez que te la hayan enviado.

Para aceptar la invitación y obtener acceso a las funciones del administrador de contraseñas, el usuario debe seguir estos pasos:

1. Abra el correo electrónico que recibió titulado **[Comience a utilizar su suscripción Bitdefender como Miembro]** y haga clic en el botón **ACTIVAR EN CENTRAL**.
2. La página de Bitdefender Central se abrirá en su navegador.
   - Si ya tiene una cuenta de usuario Bitdefender asociada al correo electrónico donde se envió la invitación, **inicie** sesión para reclamar su suscripción compartida.
   - Si no tiene una cuenta de usuario Bitdefender, haga clic en **Crear una** y regístrese con el mismo correo electrónico donde se envió la invitación para reclamar su suscripción compartida.
     - Introduce tu nombre completo
     - Introduce tu dirección de correo electrónico
     - Ingresa tu contraseña
     - Haga clic en el botón Crear cuenta y ya habrá firmado.
3. Tras iniciar sesión, haga clic en **Comenzar** en la pantalla de bienvenida que le informa de que su suscripción a Bitdefender Password Manager ya está activa.
4. Siga los pasos en pantalla que también se describen en Pasos de la Instalación (página 6).

> **Nota**
> El correo electrónico del administrador del plan se muestra en su cuenta de Bitdefender Central en la parte superior del menú del Administrador de contraseñas y en la tarjeta de suscripción, en Mis suscripciones.
>
> Si necesita ayuda con el plan compartido, póngase en contacto con ellos.

4. 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.

4.1. Compatibilidad

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

- **1Password**
- **Bitwarden**
- **Bitdefender Password Manager**
- **ByePass**
- **Chrome browser**
- **Claro**
- **Dashlane**
- **Edge browser**
- **ESET Password Manager v2**
- **ESET Password Manager v3**
- **StickyPassword**
- **Watchguard**
- **Firefox browser**
- **Gestor de contraseñas – Claro**
- **Gestor de contraseñas – SIT**
- **Gestor de contraseñas – Telnor**
- **KeePass 2.x**
- **LastPass**

- **Panda Dome Passwords**
- **PassWatch**
- **Saferpass**
- **SFR Cybersécurité**
- **SIT**
- **F-Secure**
- **Telnor**

> **Nota**
> Si en la lista proporcionada anteriormente no figura el nombre del navegador o la herramienta de gestión de contraseñas desde la que desea transferir archivos de datos, puede consultar nuestra guía online sobre cómo editar un archivo CSV de gestores de contraseñas incompatibles para poder importar su información a **Bitdefender Password Manager**: https://www.bitdefender.es/consumer/support/answer/22982/

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**.

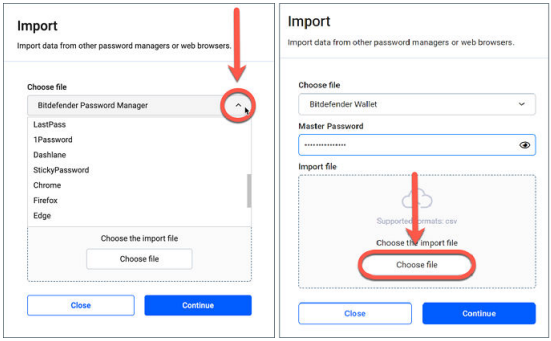
4.2. Importación a Password Manager

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. Haga clic en el icono de Password Manager en su navegador (Windows o macOS) o inicie la aplicación Password Manager (Android o iOS). En caso de que se le solicite, introduzca su **contraseña maestra**.
2. Abra el menú de Password Manager para expandir la barra lateral de la izquierda y haga clic en el elemento del menú **Ajustes**.
3. Baje hasta la sección **Datos** y haga clic en la opción **Importar datos**.
4. En el menú desplegable, seleccione el nombre de la aplicación de gestión de contraseñas o el navegador desde el que desea importar sus cuentas. Introduzca su **contraseña maestra** en el campo correspondiente y, a continuación, haga clic en **Seleccionar archivo**.



5. Explore sus carpetas hasta encontrar la ubicación en la que guardó el archivo que contiene sus nombres de usuario y contraseñas, exportado desde el otro gestor de contraseñas o navegador y, acto seguido, pulse **Continuar**.

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.

4.3. 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. Haga clic en el ícono del Administrador de contraseñas en su navegador web (en Windows o macOS) o inicie la aplicación Administrador de contraseñas (en Android o iOS). Si se le solicita, ingrese su Contraseña maestra.
2. Abra el menú de Password Manager para expandir la barra lateral de la izquierda y haga clic en el elemento del menú **Ajustes**.
3. Baje hasta la sección **Datos** y haga clic en la opción **Exportar datos**.
4. Ahora debería decidir entre las siguientes dos opciones:
   - **CSV**
   - **Archivos protegidos por contraseña**

   Seleccione la opción que prefiera y, a continuación, introduzca su contraseña maestra y haga clic en el botón **Exportar datos**.

   > **Nota**
   > Si se decanta por la opción del archivo protegido por contraseña, se le pedirá que cifre los datos de la lista de cuentas con una contraseña, para que solo usted pueda acceder a ellos en caso necesario.

5. Su aplicación o navegador guardará un archivo llamado Bitdefender Password Manager_exported_data_current-date en su sistema, en la carpeta por defecto para las descargas. Contendrá todos los datos que tiene almacenados en Bitdefender Password Manager.

Tras exportar sus datos, podrá cargarlos en el gestor de contraseñas que prefiera.

5. CARACTERÍSTICAS Y FUNCIONALIDADES

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

5.1. Gestión de contraseñas

5.1.1. Generador de contraseñas

La regla de oro para la seguridad online es usar siempre contraseñas únicas y aleatorias para cada servicio que exija la creación de una cuenta. Reutilizar las contraseñas en varias plataformas es el motivo principal del robo de identidades y de las pérdidas que conlleva que le arrebaten el control de una cuenta.

Esta característica ayuda a los usuarios a generar contraseñas seguras, complejas y únicas para cada nueva cuenta que creen en cualquier sitio online. Así, los usuarios no necesitan crear contraseñas seguras por sí mismos ni estar pendientes de no reutilizarlas en varias cuentas.

Se puede acceder al **Generador de contraseñas** desde la pestaña de la parte superior de la interfaz de Password Manager.

El generador puede configurarse para que proporcione contraseñas con una longitud **de 4 a 32 caracteres**.

Asimismo, puede especificar los tipos de caracteres que deben o no estar presentes en la contraseña generada aleatoriamente, para lo cual deberá marcar a su gusto las casillas de verificación correspondientes: **minúsculas, mayúsculas, números y caracteres especiales**.

Al pulsar el botón a la derecha de la contraseña mostrada, el generador cambiará la contraseña que ha sugerido.

Para usar la contraseña que se muestra, pulse **Utilizar contraseña**, con lo que se guardará la cadena de caracteres en el portapapeles.

> **Nota**
> Las contraseñas que ha generado anteriormente se almacenarán temporalmente en el historial de contraseñas, al cual puede acceder con el botón **Historial de contraseñas**.

5.1.2. Captura de contraseñas

Esta característica de Password Manager le pedirá que almacene todas sus nuevas contraseñas en cuanto las haya creado. Password Manager solicitará a los usuarios que almacenen sus contraseñas recién creadas, con el fin de incorporarlas inmediatamente al entorno superseguro de Bitdefender.

5.1.3. Autorrellenado inteligente

Bitdefender Password Manager puede configurarse de manera que autorrellene sus credenciales de inicio de sesión y, lo que es más importante, sus contraseñas. Sus algoritmos patentados son capaces de detectar y rellenar las credenciales en los sitios web que ha visitado anteriormente, lo que ahorra tiempo a los usuarios al iniciar sesión en un servicio.

1. En Windows o macOS, haga clic en el icono de **Password Manager** en su navegador.

   En Android o iOS, inicie la aplicación de **Password Manager**.
   En caso de que se le solicite, introduzca su **contraseña maestra**.

2. Abra el menú de Password Manager para expandir la barra lateral de la izquierda y haga clic en el elemento del menú **Ajustes**.
3. Haga clic en **Ajustes del dispositivo**.
4. Aquí verá un botón que muestra **Inhabilitar autorrellenar** o **Habilitar autorrellenar**. Este ajuste controla el funcionamiento del autorrellenado inteligente.

5.1.4. Informe de seguridad

El Informe de seguridad es una herramienta que genera informes basados en una serie de características destinadas a reforzar su seguridad digital. Determinará el nivel de seguridad de una contraseña para decirle si requiere su atención inmediata. Detectará contraseñas duplicadas y le pedirá que las cambie, para evitar el peligro de reutilizar las mismas contraseñas en varias cuentas.

El informe se centra en brindarle información sobre la higiene general de sus contraseñas: contraseñas duplicadas, contraseñas vulnerables o direcciones de correo electrónico o contraseñas que han sufrido una filtración.

Para ello, se compara localmente en su dispositivo la lista de hashes cifrados de la página web de Troy, con el fin de comprobar si contiene los hashes correspondientes a sus contraseñas. En caso de hallarse alguna coincidencia, se le notificará oportunamente para que cambie sus contraseñas y demás credenciales de inicio de sesión.

Para ver el **Informe de seguridad**, acceda a la interfaz de Password Manager y seleccione su botón en la barra superior.

5.1.5. Sincronización en otras plataformas

Guardar sus contraseñas en Bitdefender Password Manager le permitirá almacenarlas y acceder a ellas de forma segura en todos sus dispositivos Windows, Mac, Android o iOS desde Chrome, Safari, Firefox y Edge o desde aplicaciones móviles.

> **Nota**
> Bitdefender también incorpora un **modo sin conexión** para acceder a sus contraseñas, por si careciera de acceso a Internet. Gracias a ello, sus contraseñas están accesibles en todo momento y en cualquier lugar.

5.1.6. Eliminación de una entrada

Para eliminar alguna contraseña almacenada, pulse el icono de edición junto a la que desee eliminar, desde la pestaña **Cuentas**. A continuación, baje y seleccione **Eliminar**. Cuando se le pregunte si está seguro de eliminar la cuenta, seleccione **Eliminar**.

5.2. Gestión de cuentas

5.2.1. Autenticación

La autenticación en Bitdefender Password Manager se lleva a cabo mediante el **PIN** establecido durante la instalación del producto (tenga en cuenta que la característica de **Bloqueo automático** bloqueará el gestor de contraseñas o cerrará la sesión tras un período de inactividad del navegador o al cerrar la aplicación móvil).

Además, también puede autenticarse mediante datos biométricos, caso de estar disponibles, como la **huella dactilar** o el **reconocimiento facial**.

Para **habilitar o inhabilitar** la autenticación basada en los datos biométricos, haga lo siguiente:

1. En Windows o macOS, haga clic en el **Password Manager** icono en su navegador web.

   En Android o iOS, inicie el **Password Manager** solicitud.
   Si se le solicita, ingrese su Contraseña maestra.

2. Abra el menú Administrador de contraseñas para expandir la barra lateral a la izquierda y haga clic en el **Ajustes** opción del menú.
3. Haga clic en **Configuración de dispositivo**.
4. Aquí verá un botón que muestra **Inhabilitar la biometría** o **Habilitar la biometría**. Este ajuste controla el funcionamiento de la característica de autenticación basada en los datos biométricos.

5.2.2. Restablecimiento de la contraseña maestra

> **Importante**
> La característica **Cambiar la contraseña maestra** no está disponible en dispositivos móviles. La única manera de cambiar o recuperar su contraseña maestra es con la extensión de navegador de Bitdefender Password Manager en un PC con Windows o en un dispositivo macOS.

A continuación se explica cómo cambiar su **contraseña maestra** como medida de precaución y crear una nueva en Bitdefender Password Manager:

1. Una vez que haya instalado la extensión del navegador, haga clic en el icono de **Password Manager** situado en la barra de herramientas del navegador.
2. Escriba su contraseña maestra actual para desbloquear el blindaje.

> **Importante**
> Si ha olvidado su contraseña maestra actual, haga clic en la opción **Olvidé mi contraseña** de la misma pantalla. Introduzca la **clave de recuperación de 24 dígitos** que se le proporcionó durante la configuración inicial de Bitdefender Password Manager y, a continuación, escriba una nueva contraseña maestra. **Si olvida o extravía** tanto la **contraseña maestra** como la **clave de recuperación**, como último recurso, **póngase en contacto con un representante de Bitdefender para que le ayude a restablecer su cuenta**. Restablecer su cuenta **borrará todos sus datos y contraseñas** almacenados en Bitdefender Password Manager.

3. Abra el menú Administrador de contraseñas para expandir la barra lateral a la izquierda y haga clic en el **Ajustes** opción del menú.
4. Haga clic en el botón **Mi cuenta** de la sección **Cuenta**.
5. Aparecerá una ventana con información sobre su suscripción a Password Manager.
   Haga clic en el botón **Cambiar la contraseña maestra**.
6. Se le redirigirá a una nueva ventana donde podrá elegir una nueva contraseña maestra. Introduzca su contraseña maestra actual y, a continuación, escriba una nueva. La nueva contraseña maestra debe tener un mínimo de ocho caracteres y al menos una letra minúscula, una mayúscula y un número.
7. Cuando haya terminado, pulse el botón **Cambiar**.
8. Espere unos momentos hasta que Bitdefender restablezca la contraseña maestra anterior.
   ¡No salga de su navegador!
9. A continuación, se le proporcionará una nueva **clave de recuperación de 24 dígitos**. Anote su clave de recuperación en un lugar seguro y **no la pierda**. Esta clave será la única forma de acceder a sus contraseñas guardadas en Password Manager si olvidase la contraseña maestra.
   Cuando haya terminado, pulse **Cerrar**.
10. Se cerrará la sesión de Bitdefender Password Manager.
    Para desbloquear el blindaje, use la nueva contraseña maestra que acaba de establecer.

5.3. Otras funcionalidades

5.3.1. Gestión de identidades

Esta característica permite que los usuarios almacenen múltiples identidades y que Password Manager rellene automáticamente los datos en los formularios web antes de realizar una compra de manera rápida, fácil y segura.

Como todo lo demás en Password Manager, los datos confidenciales contenidos en estas identidades almacenadas están cifrados y solo a disposición del dispositivo del usuario.

Para añadir una identidad a Password Manager, haga lo siguiente:

1. En Windows o macOS, haga clic en el **Password Manager** icono en su navegador web.

   En Android o iOS, inicie el **Password Manager** solicitud.
   Si se le solicita, ingrese su Contraseña maestra.

2. Abra el menú de Password Manager para expandir la barra lateral de la izquierda y haga clic en el elemento del menú **Identidades**.

3. Pulse el botón **Añadir identidad** de la parte inferior.

4. Rellene los datos que desea almacenar y, a continuación, pulse **Guardar**.

5.3.2. Gestión de tarjetas de crédito

Esta característica le permite guardar y rellenar los datos de su tarjeta de crédito para realizar compras de forma más fácil, rápida y segura.

Para añadir una tarjeta de crédito a Password Manager, haga lo siguiente:

1. En Windows o macOS, haga clic en el **Password Manager** icono en su navegador web.

   En Android o iOS, inicie el **Password Manager** solicitud.
   Si se le solicita, ingrese su Contraseña maestra.

2. Abra el menú de Password Manager para expandir la barra lateral de la izquierda y haga clic en el elemento del menú **Tarjetas de crédito**.

3. Presiona en el **Agregar identidad** botón en la parte inferior.
4. Complete los detalles que desea almacenar y luego presione **Ahorrar**.

5.3.3. Protégeme

La característica Protégeme le permite cerrar sesión de forma remota o eliminar el historial de navegación de su equipo, tablet o dispositivo móvil. Si comparte el dispositivo con otras personas, le recomendamos que active esta característica.

Para encontrar y habilitar esta característica, haga lo siguiente:

1. En Windows o macOS, haga clic en el **Password Manager** icono en su navegador web.
   En Android o iOS, inicie el **Password Manager** solicitud.
   Si se le solicita, ingrese su Contraseña maestra.
2. Abra el menú de Password Manager para expandir la barra lateral de la izquierda y haga clic en el elemento del menú **Protégeme**.
3. Pulse el botón **Proteger todas las sesiones**.
   Si desea proteger un solo dispositivo en concreto, búsquelo en la lista de dispositivos en los que esté instalado Password Manager o en el navegador específico en que esté habilitado.

5.3.4. Notas

Las Notas seguras son una característica que actúa como un cuaderno secreto en el que puede almacenar datos confidenciales, ordenarlos y utilizar códigos de colores para verlos mejor. No solo conserva la información ordenada, sino que también la mantiene a salvo.

Para ubicar y habilitar esta función:

1. En Windows o macOS, haga clic en el **Password Manager** icono en su navegador web.
   En Android o iOS, inicie el **Password Manager** solicitud.
   Si se le solicita, ingrese su Contraseña maestra.
2. Abra el menú de Password Manager para expandir la barra lateral de la izquierda y haga clic en el elemento del menú **Notas**.
3. Pulse el botón **Añadir nota**.

Una vez que haya escrito la información que desea conservar, pulse **Guardar**.

6. 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

¿Cómo hago para que deje de aparecer la ventana emergente de Password Manager en mi solución de seguridad de Bitdefender?

La notificación de Password Manager que se mostraba en Bitdefender Total Security, Internet Security y Antivirus Plus en agosto de 2022 puede cerrarse haciendo clic en el botón “x”. La ventana “Gestione sus contraseñas con Bitdefender Password Manager” reaparecerá aleatoriamente un par de veces antes de desaparecer para siempre. Puede optar por no recibir este mensaje promocional desactivando **Notificaciones de recomendación** en los ajustes de Bitdefender.

¿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 @).

¿Cómo puedo evitar que Bitdefender me solicite la contraseña maestra cada vez que abro el navegador?

Si bloquea su dispositivo sin cerrar su navegador, Password Manager no se bloqueará y podrá acceder a sus datos cuando regrese. Como medida de seguridad, cada vez que abre el navegador debe iniciar sesión con su cuenta de Bitdefender Central y, acto seguido, introducir su contraseña maestra.

- Para anular la solicitud de inicio de sesión de Central, acceda a Ajustes y marque “Inhabilitar la pestaña de inicio de sesión al arrancar”.
- Para anular la solicitud de contraseña maestra, marque la casilla “Recordarme” en la pantalla Desbloquear su blindaje.

¿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.

Si olvidase o perdiese tanto la contraseña maestra como su clave de recuperación, como último recurso, póngase en contacto con un representante de Bitdefender para restablecer su cuenta.

Importante
Restablecer su cuenta borrará todos sus datos y contraseñas almacenados en Bitdefender Password Manager.

¿Pueden compartir varios usuarios una misma suscripción a Bitdefender Password Manager?

De momento no está disponible la posibilidad de tener varios usuarios con la misma suscripción de Password Manager, pero estamos trabajando para habilitar esta característica en un futuro próximo.

¿Qué es el modo sin conexión y cómo funciona?

El modo sin conexión se activa automáticamente cuando falla la conexión a Internet mientras se utiliza Bitdefender Password Manager. Si ya ha iniciado sesión y ha introducido su contraseña maestra, el modo sin conexión le permite acceder a sus contraseñas cuando carece de conexión a Internet.

¿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.

7. OBTENIENDO AYUDA

7.1. 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.

7.2. 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.

7.2.1. 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/.

7.2.2. 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

7.2.3. 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/.

7.3. 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 32).

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

7.3.1. Distribuidores locales

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

Para encontrar un distribuidor de Bitdefender en su país:

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

GLOSARIO

Código de activación

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

ActiveX

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

Amenaza Persistente Avanzada

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

publicidad

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

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

Archivo

Disco, cinta o directorio conteniendo ficheros almacenados.

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

Puerta trasera

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

Sector de arranque

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

virus de arranque

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

red de bots

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

Navegador

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

Ataque de fuerza bruta

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

Línea de comando

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

Galletas

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

Ciberacoso

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

Ataque de diccionario

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

Disco duro

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

Descargar

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

Correo electrónico

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

Eventos

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

hazañas

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

Falso positivo

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

Extensión de nombre de archivo

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

Heurístico

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

Tarro de miel

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

IP

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

Subprograma de Java

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

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

registrador de teclas

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

Virus de macros

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

cliente de correo

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

Memoria

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

no heurístico

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

Depredadores en línea

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

Programas empaquetados

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

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

Camino

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

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

Suplantación de identidad

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

Fotón

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

Virus polimórfico

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

Puerto

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

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

Ransomware

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

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

Archivo de informe

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

Rootkit

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

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

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

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

Script

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

Spam

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

Spyware

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

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

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

Elementos de inicio

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

Suscripción

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

Bandeja del sistema

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

TCP/IP

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

Amenaza

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

Actualización de información sobre amenazas

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

Troyano

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

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

Actualizar

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

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

Red privada virtual (VPN)

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

Gusano

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