bitwarden | Artículo del Centro de Ayuda

SEGURIDAD

Preguntas frecuentes de seguridad

Ver en el centro de ayuda:
https://bitwarden.com/help/security-faqs/

Preguntas frecuentes de seguridad

Este artículo contiene preguntas frecuentes (FAQs) sobre seguridad.

¿Por qué debería confiar en Bitwarden con mis contraseñas?

A: Puedes confiar en nosotros por algunas razones:

1. Bitwarden es un software de **código abierto**. Todo nuestro código fuente está alojado en GitHub y es gratis para que cualquiera lo revise. Miles de desarrolladores de software siguen los proyectos de código fuente de Bitwarden (¡y tú también deberías!).

2. Bitwarden es auditado **por firmas de seguridad de terceros de buena reputación** así como por investigadores de seguridad independientes.

3. Bitwarden **no almacena tus contraseñas**. Bitwarden almacena versiones cifradas de tus contraseñas que solo tú puedes desbloquear. Su información sensible se cifra localmente en su dispositivo personal antes de ser enviada a nuestros servidores en la nube.

4. **Bitwarden tiene una reputación.** Bitwarden es utilizado por millones de individuos y empresas. ¡Si hiciéramos algo cuestionable o arriesgado, estaríamos fuera de negocio!

¿Todavía no confías en nosotros? No tienes que hacerlo. El código abierto es hermoso. Puedes alojar fácilmente todo el conjunto de Bitwarden por ti mismo. Controlas tus datos. Aprende más aquí.

P: ¿Qué sucede si Bitwarden es hackeado?

A: Bitwarden toma medidas extremas para garantizar que sus sitios web, aplicaciones y servidores en la nube sean seguros. Bitwarden utiliza los servicios gestionados de Microsoft Azure para gestionar la infraestructura del servidor y la seguridad, en lugar de hacerlo directamente.

Si por alguna razón Bitwarden fuera hackeado y tus Datos estuvieran comprometidos, tu información aún estaría protegida debido a las medidas tomadas en los datos de tu caja fuerte y la contraseña maestra, como la encriptación fuerte y el hashing salteado unidireccional.

P: ¿Bitwarden puede ver mis contraseñas?

R: No.

Tus datos están completamente encriptados y/o hashados antes de salir nunca de **tu** dispositivo local, por lo que nadie del equipo de Bitwarden puede ver, leer o ingeniería inversa para llegar a tus datos reales. Los servidores de Bitwarden solo almacenan datos cifrados y hash. Para obtener más información sobre cómo se cifran sus datos, vea Cifrado.

P: ¿Se almacena mi contraseña maestra de Bitwarden localmente?

R: No.

No guardamos la contraseña maestra almacenada localmente o en la memoria. Su clave de cifrado (derivada de la contraseña maestra) se mantiene en memoria solo mientras la aplicación está desbloqueada, lo cual es necesario para desencriptar los datos en su caja fuerte. Cuando la caja fuerte está bloqueada, estos datos se eliminan de la memoria.

También recargamos el proceso de renderizado de la aplicación después de 10 segundos de inactividad en la pantalla de bloqueo para asegurarnos de que todas las direcciones de memoria gestionadas que aún no han sido recogidas por la colección de basura sean purgadas. Hacemos todo lo posible para asegurar que cualquier dato que pueda estar en memoria para el funcionamiento de la aplicación solo se mantenga en memoria el tiempo que lo necesite y que esa memoria se limpie siempre que se bloquee la aplicación. Consideramos que los datos encriptados de la aplicación son completamente seguros mientras la aplicación está en un estado bloqueado.

P: ¿Qué hago si no reconozco un nuevo dispositivo que inicia sesión en Bitwarden?

A: Si la dirección IP de un nuevo dispositivo no coincide con ninguna dirección IP conocida (red doméstica, red de trabajo, red móvil, etc.), cambie su contraseña maestra y asegúrese de que el inicio de sesión en dos pasos esté habilitado para su cuenta. También deberías desautorizar las sesiones desde la página de **Ajustes de la cuenta** de tu caja fuerte web para forzar el cierre de sesión en todos los dispositivos. Si crees que los elementos de tu caja fuerte podrían estar comprometidos, deberías cambiar tus contraseñas.

P: ¿Con qué cumple Bitwarden? ¿Qué certificaciones tienes?

A: Bitwarden cumple con las siguientes políticas:

- **RGPD.** Lee más aquí.
- **CCPA.** Lee más aquí.
- **HIPAA.** Lee más aquí.
- **SOC 2 Tipo 2.** Lee más aquí.
- **SOC 3.** Lee más aquí.

Para obtener más información, por favor visite nuestra página de Seguridad y Cumplimiento.

P: ¿Cómo cumple Bitwarden con los requisitos de cumplimiento europeos?

A: Bitwarden cumple con el RGPD y utiliza mecanismos de transferencia de información aprobados, incluyendo las Cláusulas Contractuales Estándar (CCE) de la UE de conformidad con el Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo aprobado por la Decisión de Ejecución de la Comisión Europea (UE) 2021/914 del 4 de junio de 2021, tal como se establece actualmente en https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj. Para clientes de negocios y de empresa, Bitwarden puede ejecutar el Acuerdo de Protección de Datos de Bitwarden.

Los servidores en la nube de Bitwarden están actualmente alojados en Microsoft Azure dentro de los Estados Unidos y la Unión Europea. Hoy Bitwarden sirve a millones de usuarios, incluyendo clientes gubernamentales y de empresa en toda Europa y el mundo, con esta infraestructura.

Para los clientes que necesitan un control total sobre la residencia de los datos, Bitwarden puede ser alojado de manera privada en su propia infraestructura.

Todos los datos de la caja fuerte almacenados en Bitwarden, independientemente de si están en la nube o autoalojados, están cifrados de extremo a extremo y no son accesibles por nadie excepto el usuario de Bitwarden. Con esta arquitectura de cifrado de extremo a extremo y de conocimiento cero, incluso Bitwarden no puede acceder a tus datos.

Para obtener una lista completa de las certificaciones de seguridad y cumplimiento de Bitwarden, por favor visite https://bitwarden.com/compliance/.

¿Qué servicios, bibliotecas o identificadores de terceros se utilizan en mi cuenta de Bitwarden?

A: En las aplicaciones móviles, Firebase Cloud Messaging (a menudo confundido con un rastreador) se utiliza solo para notificaciones push relacionadas con la sincronización y no realiza absolutamente ninguna función de seguimiento. Microsoft Visual Studio App Center se utiliza para el informe de fallos en una variedad de dispositivos móviles. En la caja fuerte web, los scripts de Stripe y PayPal se utilizan solo para el procesamiento de pagos en las páginas de pago.

Para aquellos que prefieren excluir toda comunicación de terceros, Firebase y Microsoft Visual Studio App Center se eliminan por completo de la construcción de F-Droid. Además, desactivar las notificaciones push en un servidor de Bitwarden autoalojado deshabilitará el uso del servidor de retransmisión de notificaciones.

La aplicación Android de Bitwarden también incluye la capacidad de desactivar el informe de fallos en los ajustes.

Bitwarden toma en serio la seguridad y la privacidad del usuario. Bitwarden mantiene una encriptación segura de extremo a extremo con cero conocimiento de tu clave de encriptación. Como una empresa centrada en el código abierto, invitamos a cualquiera a revisar nuestras implementaciones de biblioteca en cualquier momento en GitHub.

P: ¿Cómo requiero inicio de sesión de dos pasos para mi organización Bitwarden?

R: Utilice una política empresarial , incluida con una suscripción de organización empresarial. También puedes habilitar la integración de Duo MFA para hacer cumplir 2FA/MFA para tu organización. Para obtener más información, consulte Inicio de sesión en dos pasos a través de Duo.

P: ¿Cuáles son las opciones de certificado para una instancia autoalojada de Bitwarden?

A: Vea Opciones de Certificado para una lista completa e instrucciones.

P: ¿Cómo verifica Bitwarden los cambios de código?

A: La confianza en la seguridad de nuestros sistemas es de suma importancia para Bitwarden. Todos los cambios de código propuestos son revisados por uno o más miembros no autores del equipo antes de que puedan fusionarse en cualquier base de código. Todo el código pasa por múltiples pruebas y entornos de control de calidad antes de la producción. Bitwarden ha implementado un informe SOC2 para auditar y validar nuestros procedimientos internos. Como se menciona en el informe, nuestros Equipos están sujetos a rigurosos controles de antecedentes y exhaustivos procesos de entrevista. Bitwarden, al ser un producto de código abierto, también da la bienvenida a la revisión de pares de nuestro código en cualquier momento. El equipo de Bitwarden se esfuerza por hacer todo lo que podemos para mantener a nuestros usuarios cómodos, y mantener sus datos seguros.

P: ¿Cuánto tiempo guarda Bitwarden la información de la sesión en caché?

A: ¡Gran pregunta! La respuesta depende de la pieza particular de información y la aplicación del cliente:

- Las sesiones de caja fuerte sin conexión expirarán después de 30 días.
  - **Excepto** las aplicaciones de clientes móviles, que caducan a los 90 días.
- El inicio de sesión en dos pasos y las selecciones de **Recuérdame** expirarán después de 30 días.
- El caché de sincronización del Conector de Directorio se borrará después de 30 días.
- Las invitaciones de la organización expirarán después de 5 días. Los clientes autoalojados pueden configurar esto usando una variable de entorno.

P: ¿Cómo valido la suma de comprobación de una aplicación Bitwarden?

R : Primero, tome el archivo yaml `más reciente` para la versión relevante (por ejemplo, `Latest-linux.yml`) y el paquete de versión correspondiente (por ejemplo, `Bitwarden-1.33.0-amd64.deb`). Genera un hash SHA512 del paquete de lanzamiento descargado (por ejemplo, `sha512sum Bitwarden-1.33.0-amd64.deb`) y convierte el valor Hex generado a Base64. Compare el valor Base64 calculado con el valor `sha512:` del archivo yaml para validar.

P: ¿Cómo hago una divulgación de seguridad o informe a Bitwarden?

R : Bitwarden cree que trabajar con investigadores de seguridad de todo el mundo es crucial para mantener seguros a nuestros usuarios. Si cree que ha encontrado un problema de seguridad en nuestro producto o servicio, le animamos a que envíe un informe a través de nuestro Programa HackerOne. Damos la bienvenida a trabajar con usted para resolver el problema de manera rápida. Obtenga más información sobre nuestra política de divulgación .

¿Por qué mi caja fuerte web va a web-vault.pages.dev?

R : `web-vault.pages.dev` es un subdominio exclusivo de Bitwarden que utiliza Cloudflare Pages. Esta URL puede aparecer a los usuarios cuando Cloudflare está experimentando problemas con DNS. Siempre debes estar alerta ante los intentos de phishing comprobando la URL antes de ingresar tu nombre de usuario y contraseña maestra, sin embargo, `web-vault.pages.dev` se considera seguro para iniciar sesión.

P: ¿Cómo puedo proteger mi cuenta de Bitwarden de los ataques de fuerza bruta?

R: Un ataque de fuerza bruta se produce cuando un actor malintencionado recorre una combinación de contraseñas cortas y débiles en un intento de obtener acceso a su cuenta. Bitwarden ofrece algunas formas en las que puedes protegerte de estos posibles ataques:

- Ten una contraseña maestra larga y única. Bitwarden requiere un mínimo de 12 caracteres para aumentar la seguridad de la cuenta.
- Configura 2FA en todas las cuentas de Bitwarden para agregar una capa adicional de seguridad.
- Bitwarden requerirá verificación CAPTCHA después de 9 intentos fallidos de inicio de sesión desde un dispositivo desconocido.

Preguntas sobre aplicaciones específicas del cliente

¿Qué datos utiliza Bitwarden de las aplicaciones del cliente?

A: Bitwarden utiliza datos administrativos para proporcionarte el servicio de Bitwarden. Como indican algunos informes de **Privacidad de la Aplicación**, los usuarios proporcionan la siguiente información al crear una cuenta:

- Tu nombre (opcional).
- Su dirección de correo electrónico (utilizada para la verificación de correo electrónico, administración de cuenta y comunicación entre usted y Bitwarden).

Además, se asigna a su dispositivo una GUID específica del dispositivo generada por **Bitwarden** (a veces se hace referencia a ella como ID del dispositivo). Esta GUID se utiliza para alertarte cuando un nuevo dispositivo inicia sesión en tu caja fuerte.

P: ¿Puedes explicar la seguridad de la aplicación electron?

R: Un artículo que se comparte con frecuencia sugiere una falla en las aplicaciones electrónicas; sin embargo, el ataque al que se hace referencia requiere que un usuario tenga una máquina comprometida, lo que por supuesto permitiría a un atacante malintencionado comprometer los datos de esa máquina. Mientras no tengas ninguna razón para creer que el dispositivo que estás utilizando ha sido comprometido, tus datos están seguros.

¿Cómo asegura Bitwarden las extensiones de navegador?

R: Las extensiones son seguras de usar si se desarrollan correctamente. Debido a la naturaleza de cómo funcionan las extensiones de navegador, siempre existe la posibilidad de que surja un error. Tomamos extremo cuidado y precaución cuando estamos desarrollando nuestras extensiones y complementos, mantenemos nuestros ojos y oídos atentos a todo lo que sucede en la industria, y realizamos auditorías de seguridad para mantener muchos ojos en todo.

¿Para qué está pidiendo permiso la extensión del navegador?

R: Durante la instalación, la extensión del navegador le pedirá permiso para acceder a su portapapeles para poder utilizar la función de borrado programado del portapapeles (a la que se accede en el menú **Opciones**).

Cuando esta **funcionalidad opcional** está habilitada, la limpieza del portapapeles borrará cualquier entrada de Bitwarden realizada por o rellenada en un intervalo configurable. El acceso al portapapeles permite que Bitwarden haga esto sin eliminar un elemento del portapapeles no asociado con la aplicación Bitwarden al verificar el último elemento copiado contra el último elemento copiado de su caja fuerte. Por favor, toma nota, esta funcionalidad está **desactivada por defecto**.

A: ¿Qué permisos de aplicación solicita la aplicación móvil?

A: Las aplicaciones de Bitwarden para Android e iOS pueden pedir los siguientes permisos mientras estás utilizando la aplicación:

Permiso	Razón
¿Permitir a Bitwarden tomar fotos y grabar video?	Para escanear códigos QR para el inicio de sesión de dos pasos o autenticación de Bitwarden.
¿Permitir a Bitwarden acceder a las fotos y medios en su dispositivo?	Para crear adjuntos o Enviar desde un archivo guardado en tu dispositivo.

Los permisos básicos adicionales requeridos por Bitwarden están listados en la tienda Google Play.

¿Por qué la extensión del navegador necesita el permiso de nativeMessaging?

R: La versión 1.48.0 de la extensión del navegador permite el desbloqueo biométrico para las extensiones del navegador .

Este permiso, también conocido como `nativeMessaging`, es seguro aceptar y permite que la extensión del navegador se comunique con la aplicación de escritorio de Bitwarden, lo cual es necesario para habilitar desbloquear con biométrica.

Tenga en cuenta que cuando su navegador se actualice a esta versión, se le puede pedir que acepte un nuevo permiso llamado "comunicarse con aplicaciones nativas cooperativas" (en navegadores basados en Chromium), o "intercambiar mensajes con programas que no sean Firefox". Si no aceptas este permiso, la extensión permanecerá desactivada.

P: ¿Bitwarden cumple con FIPS?

R: Bitwarden utiliza criptografía y bibliotecas compatibles con FIPS 140 , y la mayoría de las instalaciones FIPS 140 de Bitwarden aprovechan la opción de autohospedaje para facilitar las evaluaciones (por ejemplo, la certificación del modelo de madurez cibernética). La plataforma Bitwarden no ha realizado ninguna certificación FIPS en este momento. Las consultas son bienvenidas a través de la página de contáctenos.

P: ¿Puedo restringir el acceso a Bitwarden a ciertos dispositivos?

A: Utilizando el autoalojamiento, puedes usar configuraciones personalizadas de firewall y NGINX, así como control de acceso VPN/VLAN para determinar los tipos de dispositivo y/o acceso de capa de red para tu instancia de Bitwarden. También puede utilizar otras herramientas, como certificados a nivel de dispositivo, para controlar el acceso específico del dispositivo a la instancia de Bitwarden.

P: ¿Bitwarden tiene una aplicación portátil?

R: ¡ Sí! La aplicación de escritorio Bitwarden está disponible para Windows como un `.exe` portátil que se puede descargar aquí. La aplicación portátil es adecuada para entornos o escenarios **siempre sin conexión** donde no se desea actualizar automáticamente la aplicación. La aplicación portátil **no se actualizará por sí misma**.

P: ¿Las opciones de acceso al sitio interferirán con la extensión de Bitwarden para el navegador?

R: La configuración de acceso al sitio para la extensión del navegador Bitwarden debe establecerse en **En todos los sitios** o en **Sitios específicos** con el servidor Bitwarden agregado a la lista, para que la extensión del navegador funcione correctamente. Establecer el acceso al sitio en **Al hacer clic** restringirá la capacidad de Bitwarden para obtener Datos del servidor de Bitwarden, lo cual es fundamentalmente necesario para guardar o actualizar las credenciales.