

Seguridad y cumplimiento de Bitwarden

Bitwarden imagina un mundo en el que nadie sea pirateado. Esto se refleja en el firme compromiso de Bitwarden con la seguridad, la privacidad y el cumplimiento de las normas internacionales.

Obtén la vista interactiva completa en
<https://bitwarden.com/es-la/compliance/>



Privacidad y seguridad de los productos Bitwarden

Auditoría por terceros

Expertos externos revisan regularmente los productos de Bitwarden, garantizando una seguridad sólida y fiable.

Cifrado de extremo a extremo con conocimiento cero

Protegido con una fuerte encriptación, nadie tiene acceso a la información de su bóveda, ¡ni siquiera Bitwarden!

Cumplimiento de las normas de privacidad y seguridad

Consiga que sus equipos internos de TI y seguridad aprueben rápidamente los productos Bitwarden con el cumplimiento de las normativas del sector.

Confianza y transparencia impulsadas por el código abierto

Una base de código abierto permite que la seguridad de los productos Bitwarden sea fácilmente auditada por investigadores de seguridad independientes, empresas de seguridad notables y la comunidad Bitwarden.

Arquitectura de código abierto de confianza

El código base de Bitwarden en GitHub es revisado y auditado regularmente por millones de entusiastas de la seguridad y miembros activos de la comunidad Bitwarden.

Evaluación del código fuente

Bitwarden realiza auditorías anuales del código fuente y pruebas de penetración para cada cliente, incluyendo la web, la extensión del navegador y el escritorio, además de la aplicación principal y la biblioteca.

Evaluación de seguridad de red

Bitwarden realiza evaluaciones anuales de la seguridad de la red y pruebas de penetración por parte de empresas de seguridad de renombre.

Recompensa por fallos de HackerOne

Los investigadores de seguridad independientes son recompensados por enviar posibles problemas de seguridad.

Proteja sus datos

Como gestor de contraseñas y proveedor de seguridad de credenciales, Bitwarden utiliza medidas de seguridad y métodos de cifrado de confianza para proteger los datos de los usuarios.

Cifrado de extremo a extremo con conocimiento cero

Bitwarden utiliza el cifrado de extremo a extremo para todos los datos de la bóveda, que sólo su contraseña maestra puede descifrar. Con una arquitectura de conocimiento-cero, Bitwarden no tiene la capacidad de leer ningún dato encriptado en su bóveda.

Cifrado multifactor

El cifrado multifactor es una capa adicional de cifrado que protege la información almacenada. Esto hace prácticamente imposible que un malhechor pueda entrar en su cámara acorazada, incluso si consiguiera acceder a los datos cifrados de la misma.

Opciones de autoalojamiento

Elija desplegar y gestionar Bitwarden in situ en su red privada o infraestructura con opciones de autoalojamiento. El autoalojamiento permite a los clientes tener un control más detallado de la información almacenada.

Cumplimiento de las normas de seguridad

Bitwarden se adhiere a los estándares de seguridad de la industria con certificaciones SOC2 y SOC3 y el cumplimiento de HIPAA.

SOC2 y SOC3

Los Controles de Sistemas y Organizaciones (SOC) comprenden un conjunto de marcos de control que se utilizan para validar los sistemas y políticas de seguridad de una organización. Bitwarden cuenta con la certificación SOC2 Tipo II y SOC3.

Informes SOC2 disponibles previa solicitud.

HIPAA

Bitwarden cumple con la HIPAA y se somete anualmente a auditorías de terceros para verificar el cumplimiento de la Norma de Seguridad de la HIPAA.

ISO 27001

Bitwarden cuenta con la certificación ISO 27001 y cumple los conjuntos de controles ISO 27001 relativos a la seguridad de los datos.

Protección de datos

Bitwarden da prioridad a la protección de los datos personales de los usuarios y garantiza el cumplimiento de las principales normas de privacidad en todo el mundo.

CCPA Y CPRA

Bitwarden cumple con la Ley de Privacidad del Consumidor de California (CCPA) y la Ley de Derechos de Privacidad de California (CPRA).

RGPD

Bitwarden cumple con el GDPR, las normas vigentes de protección de datos de la UE y las Cláusulas Contractuales Tipo (CCC) de la UE.

Data Privacy Framework

Bitwarden cumple con la Ley de Privacidad del Consumidor de California (CCPA) y la Ley de Derechos de Privacidad de California (CPRA).

Cumpla las normas de seguridad con Bitwarden

Bitwarden es más que un gestor de contraseñas: es una herramienta fundamental para lograr y mantener el cumplimiento de las principales normas de seguridad del sector. Mediante el uso compartido seguro, las capacidades de supervisión, la gestión centralizada y la sólida protección de datos, Bitwarden refuerza la postura de ciberseguridad de su organización para satisfacer las necesidades de cumplimiento.

ISO 27001

La norma internacional ISO 27001 sienta las bases para crear, mantener y desarrollar sistemas de gestión de la seguridad de la información (SGSI), incluida la gestión de datos.

NERC

La North American Electric Reliability Corporation (NERC) es un organismo regulador internacional sin ánimo de lucro dedicado a establecer normas de cumplimiento que ayuden a reducir los riesgos para la red eléctrica y los sistemas de energía que prestan servicio a cientos de millones de personas en Estados Unidos, Canadá y parte de México.

Marco de Ciberseguridad de NIST

El Instituto Nacional de Normas y Tecnología (NIST) ofrece orientación y mejores prácticas para que las organizaciones las

SOC 2

Los informes de Control de Organización de Servicios 2 (SOC 2) suelen ser solicitados por clientes y socios comerciales de proveedores de soluciones externalizadas. Las empresas que deseen cumplir la norma SOC 2 pueden recurrir a un gestor de contraseñas que la cumpla para cumplir los requisitos.

NIS2

NIS2 es un conjunto de requisitos para garantizar la seguridad de las redes y los sistemas de información en toda la UE. La directiva obliga a las empresas identificadas como operadores de servicios esenciales a aplicar medidas adecuadas para mejorar la ciberseguridad y cumplir las obligaciones legales.

SOX

El cumplimiento de la Ley Sarbanes-Oxley (SOX) implica adherirse a un conjunto de requisitos de seguridad diseñados

sigan, con el fin de ayudar a las empresas, organizaciones sin ánimo de lucro y otras instituciones del sector privado a mejorar la gestión de los riesgos de ciberseguridad.

para garantizar la integridad de los informes financieros.

Modelo de madurez de la gestión de contraseñas

Este marco ayuda a las organizaciones a comprender su nivel de madurez de gestión de contraseñas –basado en sus operaciones actuales– y a identificar qué pasos son necesarios para reforzar su seguridad y mejorar su clasificación actual.

Preguntas frecuentes

- ¿Puede el equipo de Bitwarden ver mis contraseñas?

No.

Sus datos están totalmente encriptados y/o con hash antes de salir de su dispositivo local, por lo que nadie del equipo de Bitwarden puede ver, leer o realizar ingeniería inversa para llegar a sus datos reales. Los servidores de Bitwarden sólo almacenan datos cifrados y con hash. Para más información sobre cómo se cifran tus datos, consulta [Cifrado](#).

[Más información >](#)

- ¿Cómo se mantienen seguros los servidores en nube?

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 administrar la infraestructura y la seguridad de los servidores, en lugar de hacerlo directamente.

[Más información >](#)

- ¿Está Bitwarden auditado?

Bitwarden realiza periódicamente auditorías de seguridad exhaustivas a terceros con empresas de seguridad de renombre. Estas auditorías anuales incluyen evaluaciones del código fuente y pruebas de penetración en las IP, servidores y aplicaciones web de Bitwarden.

[Más información >](#)

- ¿Qué pasa si Bitwarden es pirateado?

Si por alguna razón Bitwarden fuera hackeado y sus datos quedaran expuestos, su información seguiría estando protegida gracias a la fuerte encriptación y a las medidas de [hashing unidireccional con sal](#) adoptadas sobre sus datos de bóveda y contraseña maestra.

[Más información >](#)

- ¿Dónde se almacenan mis datos en la nube?

Bitwarden procesa y almacena todos los datos de la bóveda de forma segura en la [nube de Microsoft Azure](#) en los [EE.UU.](#) o [la UE](#) utilizando servicios que son gestionados por el equipo de Microsoft. Dado que Bitwarden solo utiliza ofertas de servicio proporcionadas por Azure, no hay infraestructura de servidor que gestionar y mantener. Todo el tiempo de actividad, escalabilidad, actualizaciones de seguridad y garantías están respaldados por Microsoft y su infraestructura en la nube. Revise la documentación de [Microsoft Azure Compliance Offerings](#) para obtener más detalles.

[Más información >](#)

- ¿Por qué debería confiar mis contraseñas a Bitwarden?

Puede confiar en nosotros por varias razones:

1. Bitwarden es un software de **código** abierto. Todo nuestro código fuente está alojado en [GitHub](#) y cualquiera puede consultarlo libremente. Miles de desarrolladores de software siguen los proyectos de código fuente de Bitwarden (¡y tú también deberías hacerlo!).
2. Bitwarden es **auditado por reputadas empresas de seguridad externas**, así como por investigadores de seguridad independientes.
3. Bitwarden **no almacena sus contraseñas**. Bitwarden almacena versiones encriptadas de tus contraseñas [que sólo tú puedes desbloquear](#). Su información confidencial 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 particulares y empresas. Si hiciéramos algo cuestionable o arriesgado, ¡quedaríamos fuera del negocio!

¿Aún no confías en nosotros? No es necesario. El código abierto es hermoso. Puede alojar fácilmente toda la pila Bitwarden usted mismo. Usted controla sus datos.

[Más información >](#)

- ¿Utiliza Bitwarden un hash salado para mi contraseña?

Se utiliza PBKDF2 SHA-256 para derivar la clave de cifrado de su contraseña maestra, aunque puede elegir [Argon2](#) como alternativa. Bitwarden [aplica sal y hash](#) a su contraseña maestra con su dirección de correo electrónico **localmente**, antes de transmitirla a nuestros servidores. Una vez que un servidor de Bitwarden recibe la contraseña cifrada, se le aplica sal con un valor aleatorio criptográficamente seguro, se vuelve a cifrar y se almacena en nuestra base de datos.

[Más información >](#)

- ¿Cómo se transmiten y almacenan mis datos de forma segura en los servidores de Bitwarden?

Bitwarden **siempre** encripta y / o hash de sus datos en su dispositivo local antes de que cualquier cosa se envíe a los servidores en la nube para el almacenamiento. **Los servidores de Bitwarden sólo se utilizan para almacenar datos cifrados**. Para más información, consulte [Almacenamiento](#).

[Más información >](#)

- ¿Qué cifrado se utiliza?

Bitwarden utiliza cifrado [AES-CBC](#) de 256 bits para los datos de su bóveda, y [PBKDF2 SHA-256](#) o [Argon2](#) para derivar su clave de cifrado.

[Más información >](#)

- ¿Qué información se encripta?

Todos los datos de la bóveda son encriptados por Bitwarden antes de ser almacenados en cualquier lugar. Para saber cómo, consulte [Cifrado](#).

[Más información >](#)

- ¿Dónde se almacenan mis datos en mi ordenador/dispositivo?

Los datos almacenados en tu ordenador/dispositivo se cifran y sólo se descifran cuando desbloqueas tu bóveda. Los datos descifrados se almacenan sólo **en memoria** y **nunca se escriben en un almacenamiento persistente**.

[Más información >](#)
