bitwarden | Artículo del Centro de Ayuda

SEGURIDAD

Bitwarden Documento de Seguridad en Blanco

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

Bitwarden Documento de Seguridad en Blanco

Resumen del Programa de Seguridad y Cumplimiento de Bitwarden

Con el aumento del trabajo remoto y el uso de internet más alto que nunca, la demanda para crear y mantener docenas (si no cientos) de cuentas en línea con inicios de sesión y contraseñas es asombrosa.

Los expertos en seguridad recomiendan que utilices una contraseña diferente, generada aleatoriamente, para cada cuenta que creas. ¿Pero cómo gestionas todas esas contraseñas? ¿Y cómo se mantiene una buena higiene de contraseña en una organización?

La gestión efectiva de contraseñas es un recurso muy subutilizado en la Empresa. En el Informe Under the Hoodie 2020 de Rapid7, hacen una nota de que la gestión de contraseñas y los controles secundarios como la autenticación de dos factores están "seriamente deficientes, lo que lleva a compromisos 'fáciles'". Reutilizar o compartir contraseñas de una manera insegura deja a la Empresa vulnerable.

Para generar un cambio en una organización, los Equipos de seguridad y TI deben educar a los empleados sobre las mejores prácticas. En cuanto a la gestión de contraseñas, una de las formas más fáciles de fomentar y apoyar una buena higiene de contraseñas es implementar una solución de administración de contraseñas en su lugar de trabajo.

Bitwarden es la forma más fácil y segura de almacenar todos tus inicios de sesión, contraseñas y otra información sensible mientras convenientemente los mantiene en sincronización entre todos tus dispositivos.

Bitwarden proporciona las herramientas para crear, almacenar y compartir tus contraseñas mientras mantiene el nivel más alto de seguridad.

La solución, software, infraestructura y procesos de seguridad de Bitwarden han sido diseñados desde cero con un enfoque de defensa en profundidad y multicapa. El Programa de Seguridad y Cumplimiento de Bitwarden se basa en el Sistema de Gestión de Seguridad de la Información (ISMS) ISO27001. Definimos políticas que rigen nuestras políticas y procesos de seguridad y continuamente actualizamos nuestro programa de seguridad para ser consistente con los requisitos legales, industriales y regulatorios aplicables para los servicios que proporcionamos bajo nuestro Acuerdo de Términos de Servicio.

Bitwarden cumple con las directrices de seguridad de aplicaciones estándar de la industria que incluyen un equipo de ingeniería de seguridad dedicado e incluyen revisiones regulares del código fuente de la aplicación y la infraestructura de TI para detectar, validar y remediar cualquier vulnerabilidad de seguridad.

Este documento técnico proporciona una visión general de los principios de seguridad de Bitwarden, así como enlaces a documentos adicionales que proporcionan más detalles en áreas específicas.

Principios de Seguridad de Bitwarden

Protección de Datos del Usuario

Bitwarden utiliza las siguientes medidas de seguridad clave para proteger los datos del usuario.

Cifrado de extremo a extremo: bloquee sus contraseñas e información privada con cifrado AES-CBC de 256 bits de extremo a extremo, hash salado y PBKDF2 SHA-256. Todas las claves criptográficas son generadas y gestionadas por el cliente en sus dispositivos, y toda la encriptación se realiza localmente. Vea más detalles en la sección de Derivación de Hashing de Contraseña.

Cifrado de conocimiento cero: los miembros del equipo de Bitwarden no pueden ver sus contraseñas. Sus datos permanecen cifrados de extremo a extremo con su correo electrónico individual y su contraseña maestra. Nunca almacenamos y no podemos acceder a su contraseña maestra o sus claves criptográficas.

> **Note**
>
> La versión de mediados de 2021 de recuperación de cuenta introdujo un nuevo par de claves públicas/privadas RSA para todas las Organizaciones. La clave privada se cifra aún más con la clave simétrica preexistente de la Organización antes de ser almacenada. El par de claves se genera y se cifra en el lado del cliente al crear una nueva Organización, o para una Organización existente al:
>
> - Navegación a la pantalla Gestionar → Personas.
> - Actualizaciones a cualquier cosa en la pantalla Ajustes → Mi Organización.
> - Mejoras de un tipo de organización a otro.

Uso compartido seguro de contraseñas: Bitwarden permite compartir y administrar de forma segura datos confidenciales con usuarios de toda una organización. Una combinación de cifrado Asimétrico y Simétrico protege la información sensible mientras se comparte.

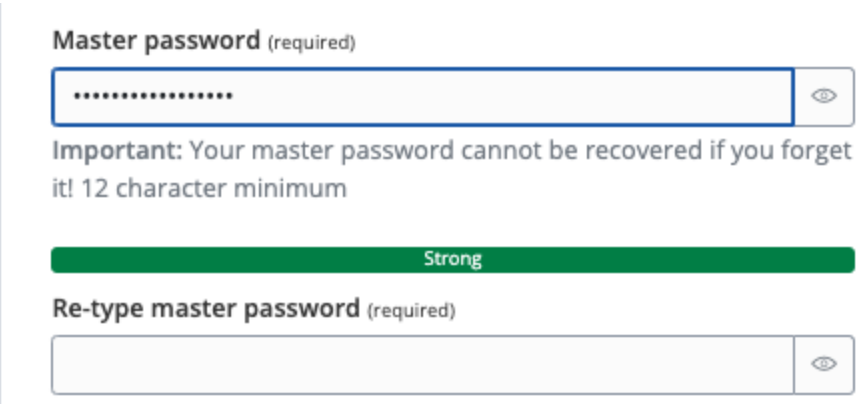
Código de fuente abierta y código disponible de fuente:
El código fuente de todos los productos de software de Bitwarden se aloja en GitHub y damos la bienvenida a todos para revisar, auditar y contribuir a la base de código de Bitwarden. El código fuente de Bitwarden es auditado por firmas de auditoría de seguridad de terceros de buena reputación, así como por investigadores de seguridad independientes. Además, el Programa de Divulgación de Vulnerabilidades de Bitwarden recluta la ayuda de la comunidad de hackers en HackerOne para hacer Bitwarden más seguro.

Privacidad por diseño: Bitwarden almacena todos sus inicios de sesión en una bóveda cifrada que se sincroniza en todos sus dispositivos. Dado que está completamente encriptado antes de que salga de su dispositivo, solo usted tiene acceso a sus datos. Ni siquiera el equipo de Bitwarden puede leer tus datos (incluso si quisiéramos). Sus datos están sellados con encriptación AES-CBC de 256 bits, hashing salteado y PBKDF2 SHA-256.

Auditoría de Seguridad y Cumplimiento: Bitwarden, de código abierto y auditado por terceros, cumple con las regulaciones AICPA SOC2 Tipo 2 / Privacy Shield, GDPR y CCPA.

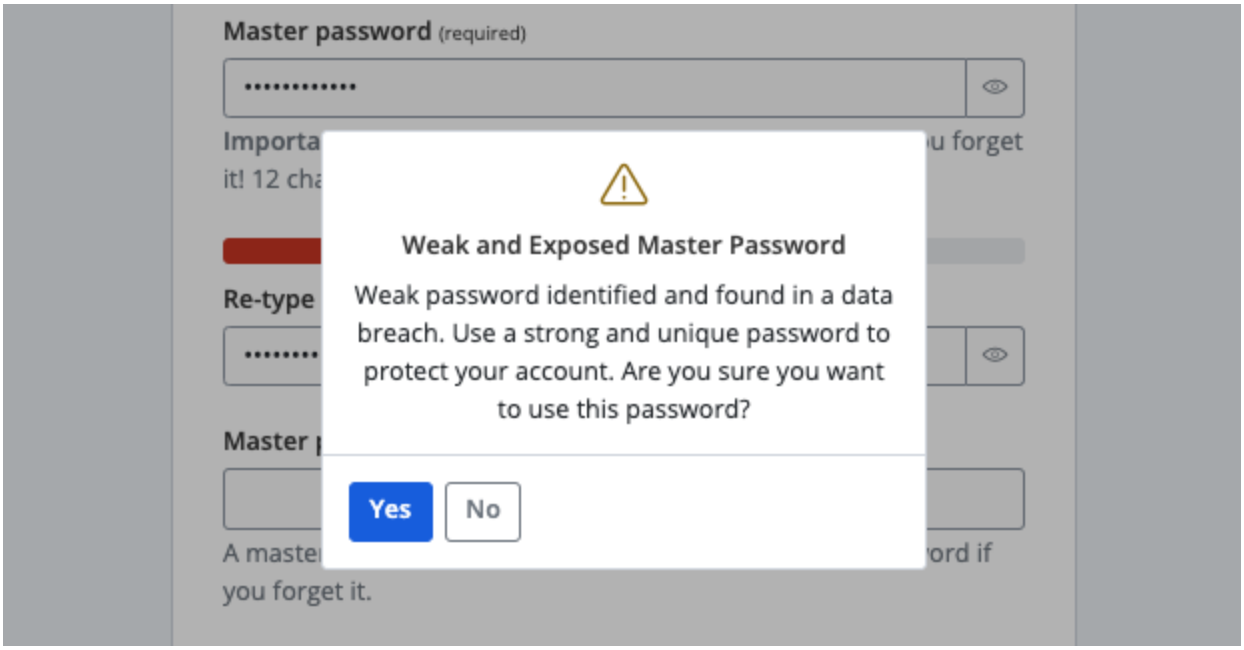
Contraseña maestra

La protección de Datos del usuario en Bitwarden comienza en el momento en que un usuario crea una cuenta y una contraseña maestra. Recomendamos encarecidamente utilizar una contraseña maestra fuerte durante el proceso de incorporación. Bitwarden incluye un Medidor de Fortaleza de Contraseña como guía que evaluará y mostrará la fortaleza general de la Contraseña Maestra que se está ingresando para fomentar una Contraseña Maestra fuerte.



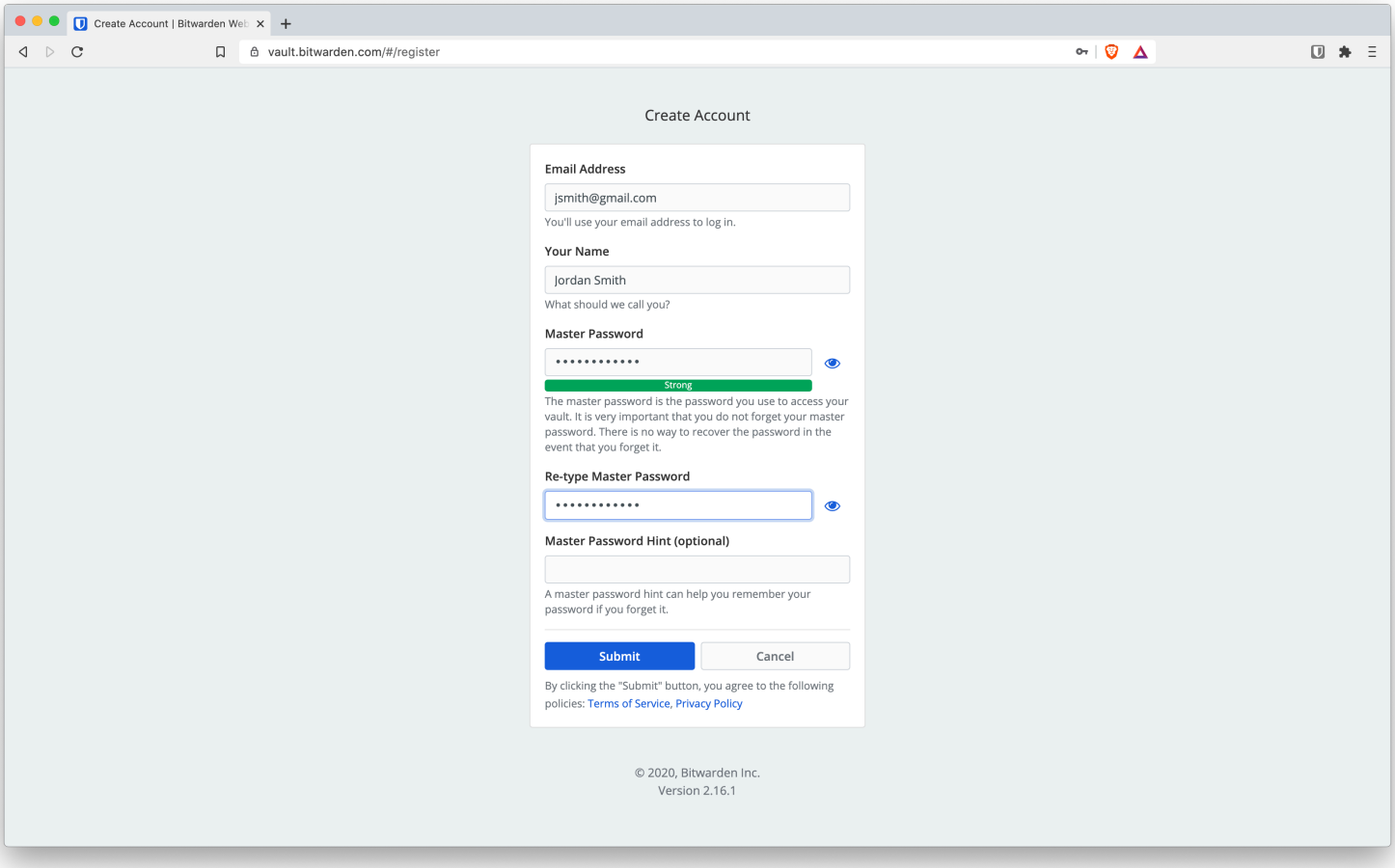
Crea una cuenta de Bitwarden

Si intentas registrarte con una contraseña débil, Bitwarden te notificará que la contraseña maestra elegida es débil. Cuando creas una cuenta de Bitwarden, también tendrás la opción de verificar las filtraciones de datos conocidas para la contraseña maestra utilizando HIBP.



Advertencia de contraseña maestra débil

Usar una contraseña maestra fuerte es para su propio beneficio de seguridad porque es el token que usa para acceder a su caja fuerte segura, donde se almacenan sus elementos sensibles. Eres responsable de mantener tu cuenta segura mientras utilizas el servicio de Bitwarden. Ofrecemos medidas adicionales, como el inicio de sesión en dos pasos, para ayudarte a mantener la seguridad de tu cuenta, pero el contenido de tu cuenta y su seguridad dependen de ti.



Elige una contraseña maestra fuerte

Leer más: Cinco mejores prácticas para la gestión de contraseñas y 3 consejos del NIST para mantener tus contraseñas seguras

Herramientas útiles: Herramienta de prueba de resistencia de contraseña de Bitwarden y Generador de contraseñas de Bitwarden

Es muy importante que nunca olvides tu contraseña maestra. La contraseña maestra se borra de la memoria después de su uso y nunca se transmite por Internet a los servidores de Bitwarden, por lo tanto, no hay forma de recuperar la contraseña en caso de que la olvides.

Esto también significa que nadie del equipo de Bitwarden puede ver, leer o ingeniería inversa para acceder a tus datos reales. Sus datos están completamente encriptados y/o hashados antes de salir nunca de su dispositivo local. Este es un paso crítico que Bitwarden toma para protegerte a ti y a tus datos.

Después de crear tu cuenta y especificar tu Contraseña Maestra, Bitwarden genera varias claves que se utilizan para proteger los datos de tu cuenta.

ⓘ Note

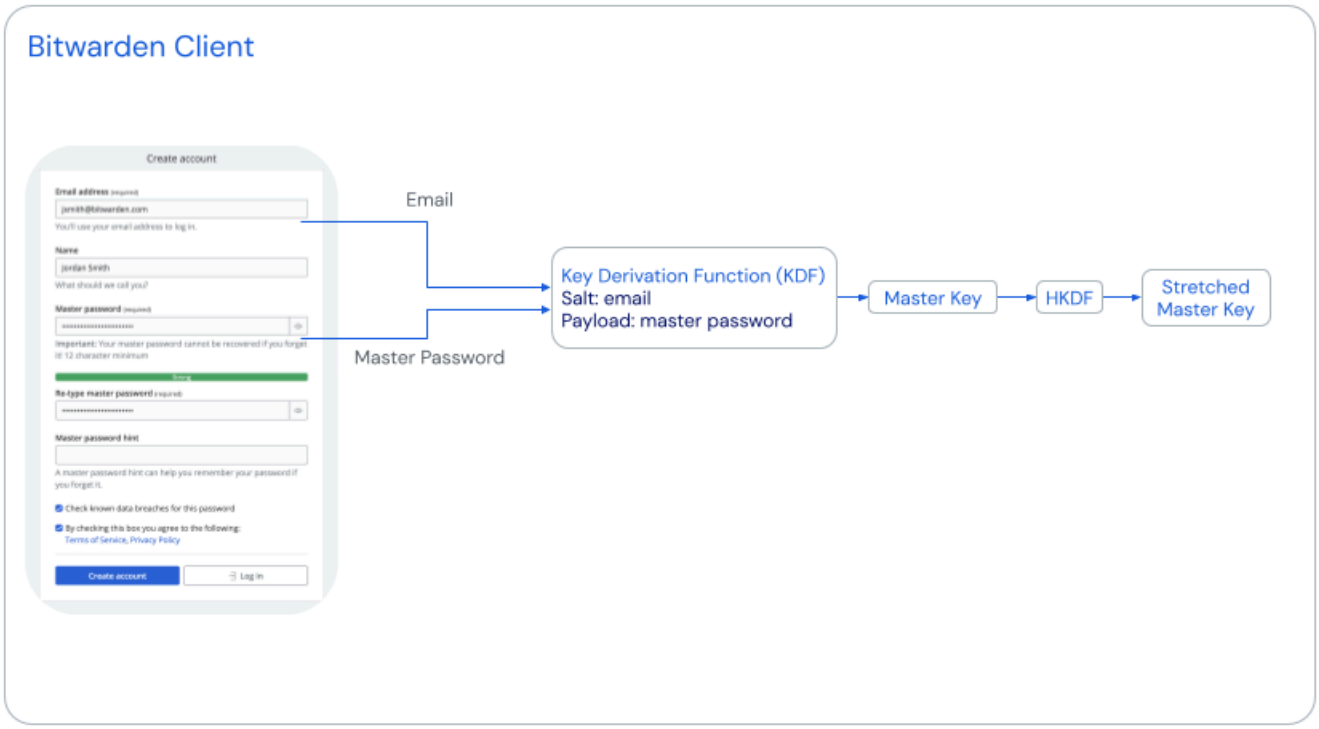
A mediados de 2021, Bitwarden introdujo la recuperación de cuenta para los planes de Empresa. Con esta opción, los usuarios y las organizaciones tienen la oportunidad de implementar una nueva política que permite a los administradores y propietarios restablecer las contraseñas de los usuarios.

Resumen del proceso de Hashing, Derivación de Clave y Encriptación de la Contraseña Maestra

Creación de Cuenta de Usuario

Cuando se envía el formulario de Crear Cuenta, Bitwarden utiliza la Función de Derivación de Clave Basada en Contraseña 2 (PBKDF2) con 600,000 rondas de iteración para estirar la Contraseña Maestra del usuario con una sal de la dirección de correo electrónico del usuario. El valor salado resultante es la Clave Maestra de 256 bits. La Clave Maestra se extiende adicionalmente a 512 bits de longitud utilizando la Función de Derivación de Clave basada en HMAC-Extract-and-Expand (HKDF). La Llave Maestra y la Llave Maestra Estirada nunca se almacenan ni se transmiten a los servidores de Bitwarden.

> **Note**
>
> En la versión 2023.2.0, Bitwarden agregó Argon2id como una opción alternativa a PBKDF2. Más información.



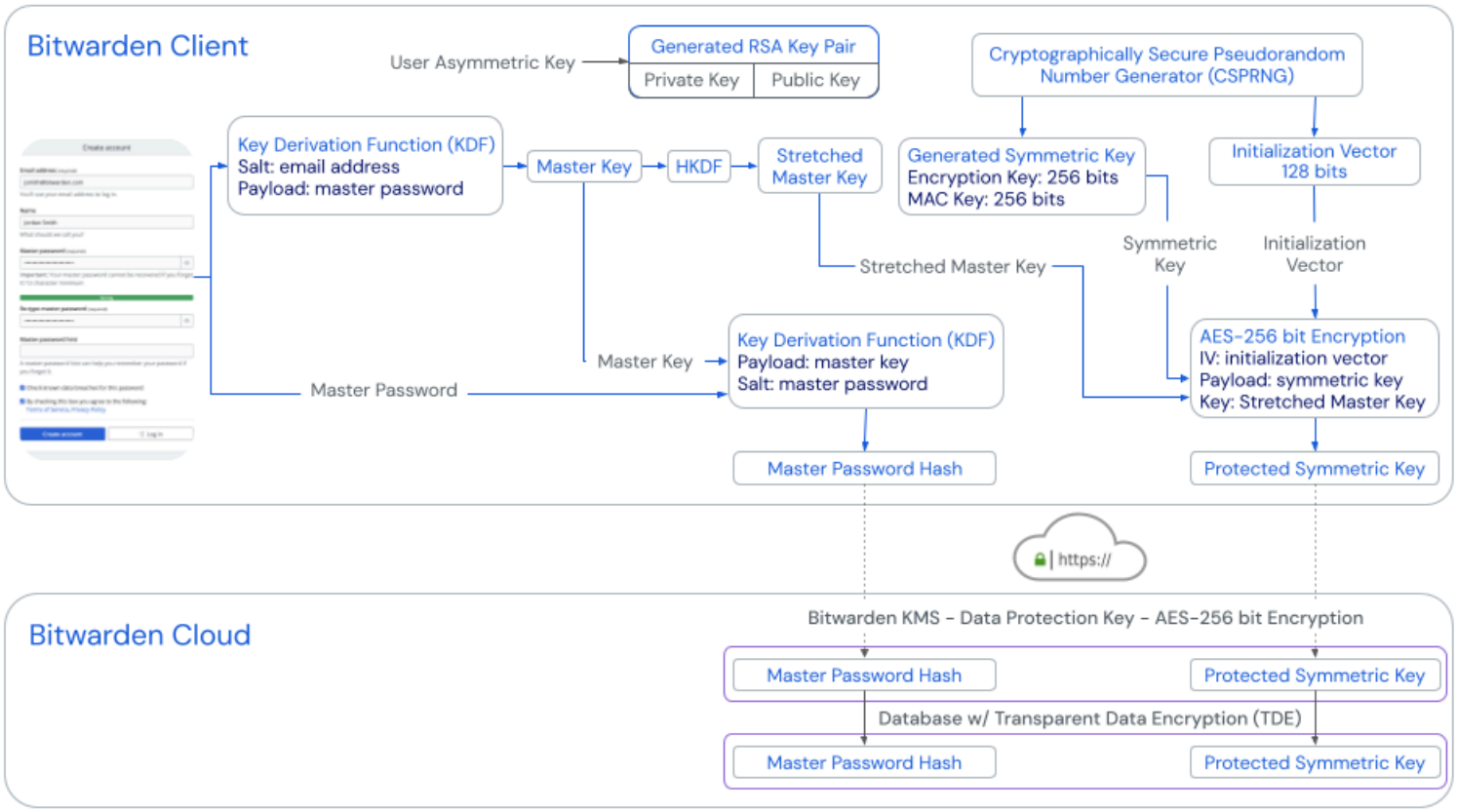
Derivación de clave basada en contraseña

Además, se genera una Clave Simétrica de 512 bits y un Vector de Inicialización utilizando un Generador de Números Pseudoaleatorios Criptográficamente Seguro (CSPRNG). La clave simétrica está cifrada con cifrado AES-256 utilizando la Clave Maestra Estirada y el Vector de Inicialización. La clave resultante se llama Clave Simétrica Protegida. La Clave Simétrica Protegida es la clave principal asociada con el usuario y enviada al servidor al crear la cuenta, y enviada de vuelta a las aplicaciones del cliente Bitwarden al realizar la sincronización.

También se genera una clave asimétrica (par de claves RSA) cuando el usuario registra su cuenta. El Par de Claves RSA Generado se utiliza si y cuando el usuario crea una Organización, la cual puede ser creada y utilizada para compartir Datos entre usuarios. Para obtener más información, consulte Compartir Datos Entre Usuarios.

También se genera un hash de la Contraseña Maestra usando PBKDF-SHA256 con una carga útil de la Clave Maestra y con una sal de la Contraseña Maestra. El hash de la contraseña maestra se envía al servidor al crear la cuenta e inicio de sesión, y se utiliza para la

autenticación de la cuenta de usuario. Una vez que se llega al servidor, el hash de la Contraseña Maestra se vuelve a cifrar utilizando PBKDF2-SHA256 con una sal aleatoria y 600,000 iteraciones. Se muestra a continuación una visión general del proceso de cifrado, derivación de claves y hash de la contraseña.



Hashing de contraseña de Bitwarden, derivación de clave y cifrado

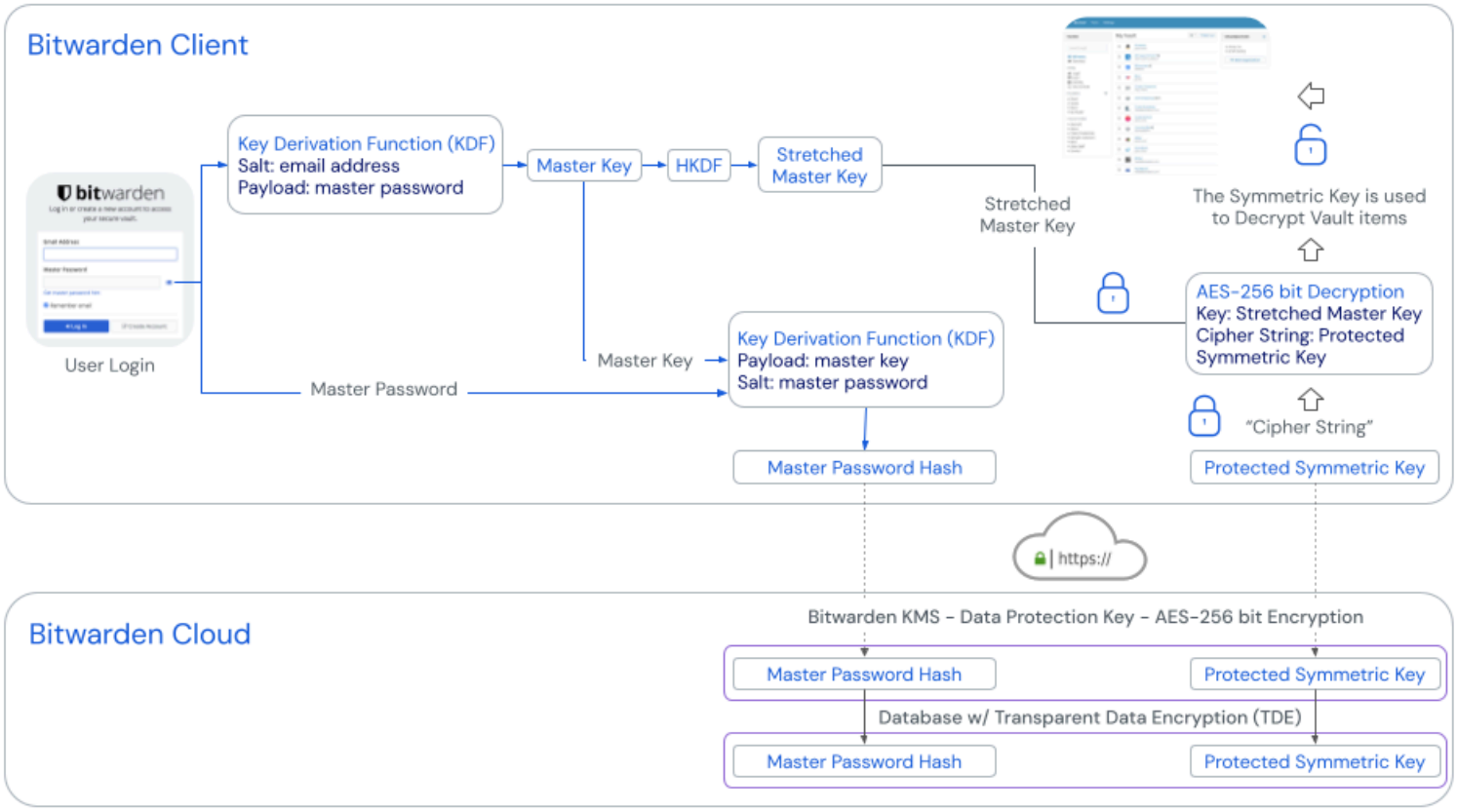
Inicio de sesión de usuario | Autenticación de usuario | Acceso a los Datos de la caja fuerte del usuario

Se requiere que primero ingrese su dirección de correo electrónico y contraseña maestra para iniciar sesión en su cuenta de Bitwarden.

A continuación, Bitwarden utiliza la Función de Derivación de Clave Basada en Contraseña 2 (PBKDF2) con un valor predeterminado de 600,000 rondas de iteración para estirar su Contraseña Maestra con una sal de su Correo Electrónico. El valor salado resultante es la Clave Maestra de 256 bits. Un hash de la clave maestra se envía al servidor al crear la cuenta e inicio de sesión, y se utiliza para autenticar la cuenta de usuario.

> **ⓘ Note**
>
> En la versión 2023.2.0, Bitwarden agregó Argon2id como una opción alternativa a PBKDF2. Más información.

La Clave Maestra se extiende adicionalmente a 512 bits de longitud utilizando la Función de Derivación de Clave basada en HMAC Extract-and-Expand (HKDF). La Clave Simétrica Protegida se descifra utilizando la Clave Maestra Estirada. La Clave Simétrica se utiliza para descifrar los Elementos de la Caja Fuerte. La desencriptación se realiza completamente en el Cliente de Bitwarden porque su Contraseña Maestra o Clave Maestra Estirada nunca se almacena ni se transmite a los servidores de Bitwarden.



Una visión general del inicio de sesión del usuario

No guardamos la Contraseña Maestra almacenada localmente o en la memoria en el Cliente de Bitwarden. Tu clave de cifrado (Clave Simétrica) se mantiene en memoria mientras la aplicación está desbloqueada. Esto es necesario para descifrar los Datos en tu caja fuerte. Cuando la caja fuerte está bloqueada, estos datos se eliminan de la memoria. Después de un cierto período de inactividad en la pantalla de bloqueo, recargamos los procesos de la aplicación para asegurarnos de que también se purguen las direcciones de memoria gestionadas que quedan. 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 la aplicación es completamente segura mientras está en un estado bloqueado.

Protección Adicional de Datos de Usuario al habilitar el inicio de sesión en dos pasos

El inicio de sesión en dos pasos (también llamado autenticación de dos factores o 2FA) es una capa extra de seguridad para tu cuenta, diseñada para asegurar que tú eres la **única** persona que puede acceder a tu cuenta, incluso si alguien descubriera tu contraseña maestra.

Como mejor práctica, recomendamos que todos los usuarios activen y utilicen el inicio de sesión de dos pasos en su cuenta de Bitwarden. Cuando se activa el inicio de sesión en dos pasos, se requiere que completes un paso secundario al iniciar sesión en Bitwarden (además de tu contraseña maestra). Por defecto, se te pedirá que completes este segundo paso cada vez, sin embargo, hay una opción de "Recordarme", que guardará tu estado de 2FA, por lo que puedes iniciar sesión sin 2FA la próxima vez en ese dispositivo en particular durante hasta 30 días.

Nota: Cambiar tu contraseña maestra o desautorizar sesiones requerirá que vuelvas a autenticar 2FA, sin importar si seleccionaste "Recuérdame" anteriormente o no.

Bitwarden admite el inicio de sesión en dos pasos utilizando los siguientes métodos:

Planes Gratis

- Usando una aplicación de autenticación (por ejemplo, 2FAS, Ravio, o Aegis)
- FIDO2 WebAuthn (cualquier llave certificada FIDO2 WebAuthn)
- Correo electrónico

Funcionalidades Premium – incluidas como parte de los Planes de Familias, Equipos y Empresa

- Duo Security con Duo Push, SMS, llamada telefónica y claves de seguridad U2F
- YubiKey (cualquier dispositivo de la serie 4/5 o YubiKey NEO/NFC)

Puedes habilitar múltiples métodos de inicio de sesión de dos pasos. Si tienes habilitados varios métodos de inicio de sesión en dos pasos, el orden de preferencia para el método predeterminado que se muestra al iniciar sesión es el siguiente: FIDO U2F > YubiKey > Duo > Aplicación de autenticación > Correo electrónico. Puedes cambiar y usar cualquier método manualmente durante el inicio de sesión, sin embargo.

Es muy importante que nunca pierdas tus códigos de recuperación de inicio de sesión de dos pasos. Bitwarden ofrece un modelo de seguridad de protección de cuenta que no admite que los usuarios pierdan su contraseña maestra o los códigos de recuperación de inicio de sesión en dos pasos. Si tienes habilitado el inicio de sesión en dos pasos en tu cuenta y pierdes el acceso a tus códigos de recuperación de inicio de sesión en dos pasos, no podrás iniciar sesión en tu cuenta de Bitwarden.

> **ⓘ Note**
>
> A mediados de 2021, Bitwarden introdujo la recuperación de cuenta para los planes de Empresa. Con esta opción, los usuarios y las organizaciones tienen la oportunidad de implementar una nueva política que permite a los administradores y propietarios restablecer las contraseñas de los usuarios.

Cambiando la Contraseña del Usuario

Su Contraseña Maestra solo puede ser cambiada desde la Caja Fuerte Web. Para obtener instrucciones específicas sobre cómo cambiar su contraseña de usuario, consulte este artículo de ayuda de Bitwarden.

Rotando la Clave de Cifrado de Tu Cuenta

Durante una operación de cambio de contraseña, también tienes la opción de rotar (cambiar) la clave de cifrado de tu cuenta. Rotar la clave de cifrado es una buena idea si crees que tu contraseña maestra anterior fue comprometida o que los datos de tu caja fuerte de Bitwarden fueron robados de uno de tus dispositivos.

> **⚠ Warning**
>
> Rotar la clave de cifrado de tu cuenta es una operación delicada, por lo que no es una opción predeterminada. Una rotación de clave implica generar una nueva clave de cifrado aleatoria para su cuenta y **volver a cifrar todos los datos de la caja fuerte** utilizando esta nueva clave. Vea detalles adicionales en este artículo.

Protección de Datos en Tránsito

Bitwarden toma la seguridad muy en serio cuando se trata de manejar tus datos sensibles. Tus datos nunca se envían a la nube de Bitwarden sin antes ser cifrados en tu dispositivo local.

Además, Bitwarden utiliza TLS/SSL para asegurar las comunicaciones entre los clientes de Bitwarden y los dispositivos de los usuarios hacia la nube de Bitwarden. La implementación de TLS de Bitwarden utiliza certificados X.509 de 2048 bits para la autenticación del servidor e intercambio de claves y un conjunto de cifrado fuerte para el cifrado masivo. Nuestros servidores están configurados para rechazar cifrados y protocolos débiles.

Bitwarden también implementa encabezados de seguridad HTTP como HTTP Strict Transport Security (HSTS), que obligará a todas las conexiones a usar TLS. Esta capa adicional de protección con HSTS mitiga los riesgos de ataques de degradación y mala configuración.

Protección de Datos en Reposo

Bitwarden siempre encripta y/o hashea tus datos en tu dispositivo local antes de que se envíen a los servidores en la nube para la sincronización. Los servidores de Bitwarden solo se utilizan para almacenar y sincronizar los Datos encriptados de la caja fuerte. No es posible obtener tus datos sin encriptar de los servidores en la nube de Bitwarden. Específicamente, Bitwarden utiliza encriptación AES de 256 bits así como PBKDF-SHA256 para asegurar tus datos.

AES es un estándar en criptografía y es utilizado por el gobierno de los EE. UU. y otras agencias gubernamentales alrededor del mundo para proteger datos de alto secreto. Con una implementación adecuada y una clave de cifrado fuerte (tu contraseña maestra), se considera que el AES es irrompible.

PBKDF-SHA256 se utiliza para derivar la clave de cifrado de su Contraseña Maestra. Entonces, esta clave se sala y se cifra para la autenticación con los servidores de Bitwarden. El recuento de iteraciones predeterminado utilizado con PBKDF2 es de 600,001 iteraciones en el cliente (este recuento de iteraciones del lado del cliente se puede configurar desde los ajustes de su cuenta), y luego 100,000 iteraciones adicionales cuando se almacena en nuestros servidores (para un total de 700,001 iteraciones por defecto).

> **Note**
>
> En la versión 2023.2.0, Bitwarden agregó Argon2id como una opción alternativa a PBKDF2. Más información.

Algunos datos cifrados, incluyendo la clave simétrica protegida de un usuario y el hash de la contraseña maestra, también son cifrados de manera transparente en reposo por la aplicación, lo que significa que se cifran y descifran nuevamente a medida que fluyen dentro y fuera de la base de datos de Bitwarden.

Bitwarden además utiliza la encriptación de datos transparente de Azure (TDE) para proteger contra la amenaza de actividad maliciosa fuera de línea realizando encriptación y desencriptación en tiempo real de la base de datos, las copias de seguridad asociadas y los archivos de registro de transacciones en reposo.

Aprende más: Cómo la encriptación de extremo a extremo allana el camino para el conocimiento cero y Qué encriptación se está utilizando

Iniciar sesión con claves de acceso y mantener el cifrado de extremo a extremo

Además de la contraseña maestra, los usuarios pueden elegir desbloquear sus cajas fuertes con una llave de paso. Este proceso aprovecha un estándar de vanguardia y una extensión para WebAuthn llamada función pseudoaleatoria o PRF, que obtiene material clave de un autenticador. Con PRF, las claves derivadas se utilizan en el cifrado y descifrado de datos almacenados en la caja fuerte del administrador de contraseñas Bitwarden y el Administrador de secretos Bitwarden, manteniendo el cifrado de conocimiento cero de extremo a extremo.

Cuando se registra una clave de acceso para iniciar sesión en Bitwarden:

1. Un **par de claves pública y privada de passkey** es generado por el autenticador a través de la API de WebAuth. Este par de claves, por definición, es lo que constituye tu contraseña.

2. Una **clave simétrica PRF** es generada por el autenticador a través de la extensión PRF de la API de WebAuthn. Esta clave se deriva de un **secreto interno** único para tu llave de acceso y una **sal** proporcionada por Bitwarden.

3. Un **par de claves públicas y privadas PRF** es generado por el cliente de Bitwarden. La clave pública PRF cifra tu **clave de cifrado de cuenta**, a la cual tu cliente tendrá acceso por virtud de estar iniciado sesión y desbloqueado, y la resultante **clave de cifrado de cuenta cifrada con PRF** se envía al servidor.

4. La **clave privada PRF** se cifra con la **clave simétrica PRF** (ver Paso 2) y la **clave privada PRF cifrada** resultante se envía al servidor.

5. Su cliente envía datos a los servidores de Bitwarden para crear un nuevo registro de credenciales de clave de paso para su cuenta. Si su clave de acceso está registrada con soporte para el cifrado y descifrado de la caja fuerte, este registro incluye:
   - El nombre de la contraseña
   - La clave pública de la contraseña
   - La clave pública PRF
   - La clave de cifrado de la cuenta cifrada con PRF
   - La clave privada cifrada con PRF

Su clave privada de contraseña, que se requiere para realizar la autenticación, solo sale del cliente en un formato cifrado.

Cuando se utiliza una clave de acceso para iniciar sesión y, específicamente, para descifrar los datos de tu caja fuerte:

1. Usando la criptografía de clave pública de la API WebAuthn, su solicitud de autenticación es afirmada y confirmada.
2. Su **clave de cifrado de cuenta cifrada con PRF** y **clave privada cifrada con PRF** se envían desde el servidor a su cliente.
3. Usando la misma **sal** proporcionada por Bitwarden y el **secreto interno** único para tu llave de paso, la **clave simétrica PRF** se recrea localmente.
4. La **clave simétrica PRF** se utiliza para descifrar tu **clave privada cifrada con PRF**, resultando en tu **clave privada PRF**.
5. La **clave privada PRF** se utiliza para descifrar tu **clave de cifrado de cuenta cifrada con PRF**, resultando en tu **clave de cifrado de cuenta**. La clave de cifrado de su cuenta se utiliza para descifrar los datos de su caja fuerte.

Cómo se Aseguran los Elementos de la Caja Fuerte

Toda la información (Inicios de sesión, Tarjetas, Identidades, Notas) asociada con sus Datos almacenados en la caja fuerte está protegida con cifrado de extremo a extremo. Los elementos que eliges almacenar en tu caja fuerte de Bitwarden se almacenan primero con un elemento llamado objeto Cipher. Los objetos de cifrado están encriptados con tu Clave Simétrica Generada, que solo puede ser conocida al desencriptar tu Clave Simétrica Protegida usando tu Clave Maestra Estirada. Esta encriptación y desencriptación se realizan completamente en el cliente de Bitwarden porque su contraseña maestra o clave maestra estirada nunca se almacena ni se transmite a los servidores de Bitwarden.

Informes sanitarios de las cámaras acorazadas

Todos los planes pagados de Bitwarden vienen con informes de salud de la caja fuerte tanto para individuos como para organizaciones.

Para cajas fuertes individuales, los individuos tienen acceso a lo siguiente:

- Informe de Contraseñas Comprometidas
- Informe de Contraseñas Reutilizadas
- Informe de Contraseñas Débiles
- Informe de Sitios Web No Seguros
- Informe de 2FA Inactivo

- Informe de Filtración de Datos

Para los usuarios de negocios, existe un conjunto similar de informes para los elementos de la caja fuerte de la organización.

Leer más:Informe de Caja Fuerte Health

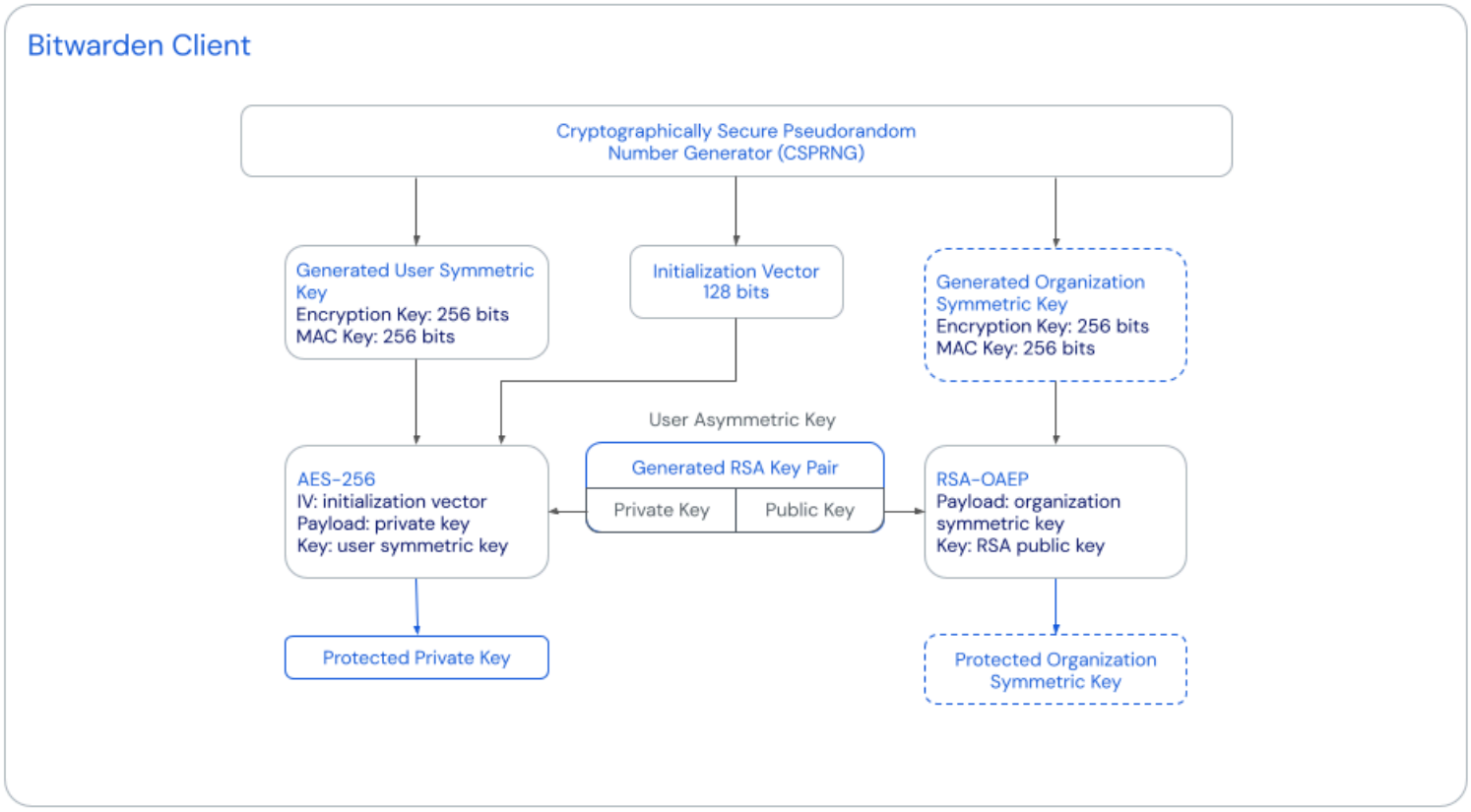
Para obtener más información sobre los registros de eventos de Bitwarden e informes externos, consulte Registros de eventos.

Importar Contraseñas y Otros Secretos a Bitwarden

Puedes importar fácilmente tus datos de más de 40 servicios diferentes, incluyendo todas las populares aplicaciones de administrador de contraseñas, a Bitwarden. La lista completa de aplicaciones compatibles y alguna información adicional, incluyendo los pasos para solucionar problemas al importar tus datos a Bitwarden, están documentados en Centro de Ayuda de Bitwarden.

Si está exportando sus sitios desde la caja fuerte web de LastPass.com, consulte la información específica en esta nota de ayuda Importe sus datos desde LastPass.

Compartiendo Datos Entre Usuarios



Protección y intercambio de claves de la organización

La colaboración es uno de los principales beneficios de usar un administrador de contraseñas. Para habilitar el compartir, primero necesitas crear una Organización. Una organización de Bitwarden es una entidad que relaciona a los usuarios que desean compartir elementos. Una organización podría ser una familia, equipo, compañía, o cualquier otro tipo de grupo que desea compartir datos.

Una cuenta de usuario individual puede crear y/o pertenecer a muchas organizaciones diferentes, lo que te permite gestionar tus elementos desde una sola cuenta.

Puedes crear una nueva organización Bitwarden desde la caja fuerte web o solicitar que un administrador de una organización existente te envíe una invitación.

Cuando Creas una Organización

Cuando creas una Organización, se genera una clave simétrica de Organización utilizando un Generador de Números Pseudoaleatorios Criptográficamente Seguro (CSPRNG). Esta clave simétrica de la Organización es lo que se utiliza para descifrar los Datos de la caja fuerte propiedad de la Organización, por lo tanto, compartir Datos con los miembros de la Organización requiere proporcionar acceso a ella de manera segura. La clave simétrica en bruto de la organización nunca se almacena en los servidores de Bitwarden.

Tan pronto como se genera la clave simétrica de la Organización, se utiliza RSA-OAEP para cifrar la clave simétrica de la organización con la clave pública RSA del creador de la Organización. Se genera un par de claves RSA para cada usuario al crear una cuenta, independientemente de si son miembros de una Organización o no, por lo que esta clave ya existirá antes de la creación de la Organización.

> **Note**
>
> La clave privada RSA, cuyo uso se describe a continuación, se almacena cifrada con la clave de cifrado de la cuenta del usuario, por lo que los usuarios deben iniciar sesión completamente para obtener acceso a ella.

El valor resultante de esta operación se conoce como la clave simétrica de la Organización protegida y se envía a los servidores de Bitwarden.

Cuando el creador de la organización, o cualquier miembro de la organización, inicia sesión en su cuenta, la aplicación del cliente utiliza la clave privada RSA desencriptada para desencriptar la clave simétrica protegida de la Organización, resultando en la clave simétrica de la Organización. Usando la clave simétrica de la organización, los datos de la caja fuerte propiedad de la organización se descifran localmente.

Cuando los Usuarios se Unen a una Organización

El proceso para que los usuarios posteriores se unan a una organización es bastante similar, sin embargo, algunas diferencias valen la pena tomar nota.

Primero, un miembro establecido de la Organización, específicamente alguien con permiso para incorporar a otros usuarios, confirma al usuario a la Organización. Este miembro establecido, en virtud de haber iniciado sesión en su cuenta y haber pasado por el proceso de descifrado de Datos de la organización descrito en la sección anterior, tiene acceso a la clave simétrica descifrada de la organización.

Entonces, cuando se confirma el nuevo usuario, el cliente del miembro establecido se conecta con los servidores de Bitwarden, recupera la clave pública RSA del nuevo usuario, que se almacena en los servidores de Bitwarden en el momento de la creación de la cuenta, y cifra la clave simétrica de la organización descifrada con ella. Esto resulta en una nueva clave simétrica de Organización protegida que se envía a los servidores de Bitwarden y se almacena para el nuevo miembro.

> **Note**
>
> Cada clave simétrica de la Organización protegida es única para su usuario, pero cada una se descifrará a la misma clave simétrica de la Organización requerida cuando se descifre con la clave privada RSA específica de su usuario.

Cuando el nuevo usuario inicia sesión en su cuenta, la aplicación del cliente utiliza la clave privada RSA desencriptada para desencriptar la nueva clave simétrica de la Organización protegida, resultando en la clave simétrica de la organización. Usando la clave simétrica de la organización, los datos de la caja fuerte propiedad de la organización se descifran localmente.

Leer más: ¿Qué son las organizaciones?

Controles de Acceso y Gestionar Colecciones de Bitwarden

A medida que el uso de Bitwarden por parte de su organización crece, es útil tener usuarios que puedan gestionar colecciones de forma independiente, sin requerir acceso a todo dentro de la caja fuerte de la organización.

Gestionar Colecciones y Grupos es una forma sencilla de separar, otorgar o limitar el acceso a elementos de la caja fuerte en Bitwarden, controlando así la visibilidad del usuario de los recursos.

Una lista completa de roles y control de acceso está documentada en la sección Tipos de Usuario y Control de Acceso del Centro de Ayuda de Bitwarden.

Leer más: Sobre las Colecciones

Registros de Eventos

Los registros de eventos contienen información detallada con fecha y hora sobre qué acciones o cambios han ocurrido dentro de una organización. Estos registros son útiles para investigar cambios en las credenciales o configuración y son muy útiles para la investigación de rastros de auditoría y propósitos de resolución de problemas.

Información adicional sobre Registros de Eventos se documenta en el Centro de Ayuda de Bitwarden. Los registros de eventos están disponibles solo para los planes de Equipos y Negocios.

Para recopilar más datos, los planes con acceso a API pueden usar la API de Bitwarden. Las respuestas de la API contendrán el tipo de evento y los datos relevantes.

Integración de SIEM y Sistemas Externos

Para sistemas de Gestión de Información y Eventos de Seguridad (SIEM) como Splunk, al exportar datos de Bitwarden, se puede utilizar una combinación de datos de la API y la ILC para recopilar datos.

Este proceso se describe en la nota del centro de ayuda sobre **Registros de eventos de la organización** bajo Integraciones de SIEM y Sistemas Externos.

Protección de la Cuenta y Evitación del Bloqueo

Hoy, para los planes Básico, Premium, Familias y Equipos, Bitwarden ofrece protección de cuenta con un modelo de seguridad que no admite que los usuarios pierdan sus contraseñas o códigos de recuperación de inicio de sesión en dos pasos.

Bitwarden no puede restablecer las contraseñas de los usuarios ni puede desactivar el inicio de sesión en dos pasos si se ha habilitado en su cuenta. Los propietarios o administradores de cuentas de Familias y Equipos no pueden restablecer las contraseñas de los usuarios. Consulte la siguiente sección para obtener detalles sobre los planes de la Empresa.

> ⚠ **Warning**
>
> Los usuarios que pierden su contraseña maestra, o que pierden su código de recuperación de inicio de sesión en dos pasos, necesitarán eliminar su cuenta y comenzar de nuevo.

Para mitigar estos posibles problemas, Bitwarden recomienda lo siguiente para la protección de la cuenta y la prevención de bloqueos.

Contraseña Maestra
Identifique una forma para que pueda retener y poder recuperar su Contraseña Maestra en caso de que la olvide. Esto puede incluir escribirlo y colocarlo en una caja fuerte, o en un lugar seguro.

Usa una pista para la contraseña maestra
Si es útil, use la pista de la contraseña maestra proporcionada por Bitwarden al registrarse. O configure una pista en cualquier momento a través de los ajustes en la caja fuerte web.

Gestión de organización
Para las organizaciones, tenga varios administradores que puedan acceder y gestionar la organización.

Código de recuperación de inicio de sesión en dos pasos
Si eliges o tu Organización te requiere configurar el inicio de sesión en dos pasos, asegúrate de acceder y conservar tu Código de recuperación y almacénalo en un lugar igual de seguro que tu Contraseña maestra.

Recuperación de Cuenta en Planes de Empresa

A mediados de 2021, Bitwarden introdujo recuperación de cuenta para planes de Empresa. Con esta opción, los usuarios y las organizaciones tienen la oportunidad de implementar una nueva política que permite a los Administradores y Propietarios restablecer las contraseñas de los usuarios.

Seguridad de la Plataforma en la Nube y la Aplicación Web de Bitwarden

Resumen de la Arquitectura de Bitwarden

Bitwarden procesa y almacena todos los datos de manera segura en la nube de Microsoft Azure utilizando servicios que son gestionados por el equipo de Microsoft. Dado que Bitwarden solo utiliza las ofertas de servicio proporcionadas por Azure, no hay infraestructura de servidor para gestionar y mantener. Todas las actualizaciones de tiempo de actividad, escalabilidad y seguridad, parches y garantías están respaldadas por Microsoft y su infraestructura en la nube.

Actualizaciones de Seguridad y Parches

El equipo de Microsoft gestiona la actualización de OS en dos niveles, los servidores físicos y las máquinas virtuales de invitados (VMs) que ejecutan los recursos del Servicio de Aplicaciones Azure. Ambos se actualizan mensualmente, lo que se alinea con el horario mensual del Martes de Parches de Microsoft. Estas actualizaciones se aplican automáticamente, de una manera que garantiza el SLA de alta disponibilidad de los servicios de Azure.

Leer Más: Parcheando en Azure App Service o SLA para App Service

Para obtener información detallada sobre cómo se aplican las actualizaciones, lea aquí

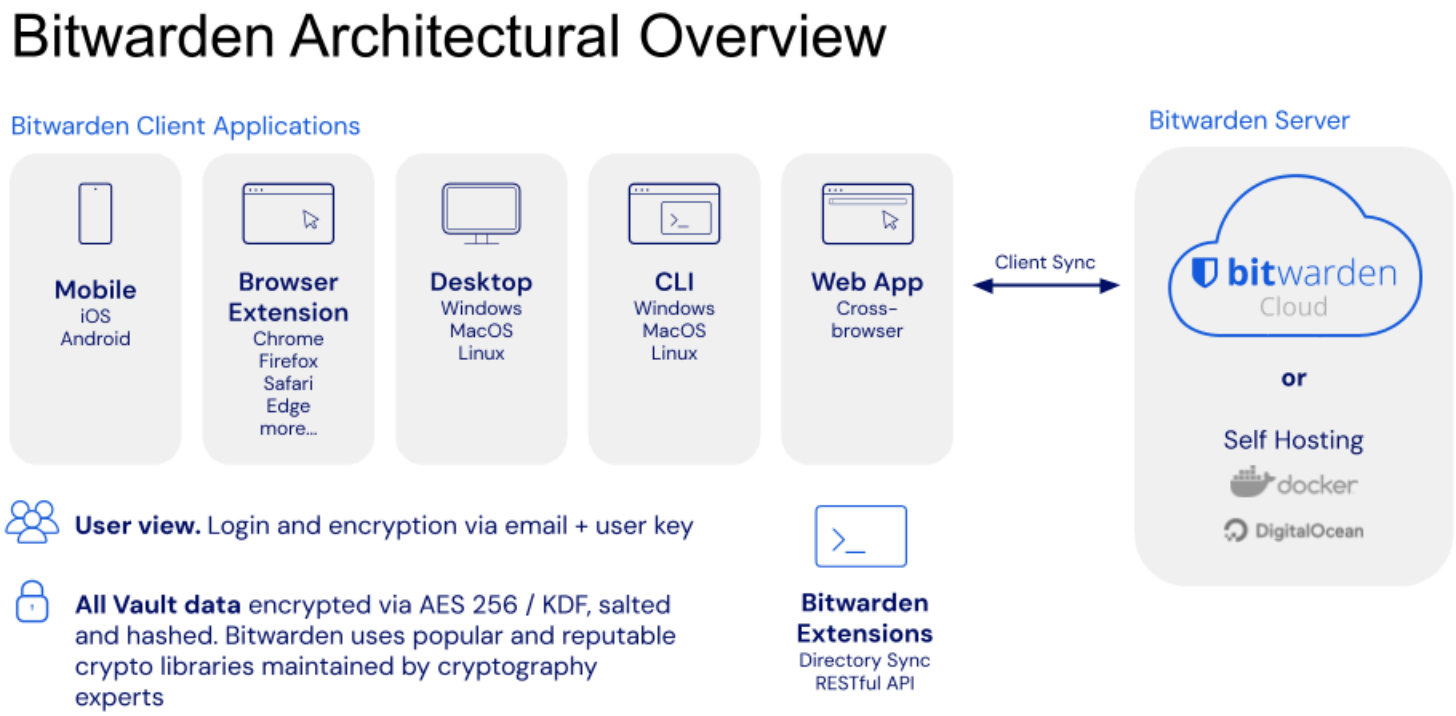


Figura: Una visión general de la arquitectura de Bitwarden

Controles de Acceso de Bitwarden

Los empleados de Bitwarden tienen una formación y experiencia significativas para el tipo de Datos, sistemas y activos de información con los que diseñan, arquitectan, implementan, gestionan, apoyan e interactúan.

Bitwarden sigue un proceso de incorporación establecido para garantizar que se asigna y se mantiene el nivel de acceso apropiado. Bitwarden ha establecido niveles de acceso que son apropiados para cada rol. Todas las solicitudes, incluyendo cualquier solicitud de cambio de acceso, necesitan ser revisadas y aprobadas por el gerente que debe gestionarlas. Bitwarden sigue una política de mínimo privilegio que otorga a los empleados el nivel mínimo de acceso requerido para completar sus deberes. Bitwarden sigue un proceso de desvinculación establecido a través de los Recursos Humanos de Bitwarden que revoca todos los derechos de acceso al terminar.

Ciclo de Vida del Software y Gestión de Cambios

Bitwarden evalúa los cambios en la plataforma, las aplicaciones y la infraestructura de producción para minimizar el riesgo y dichos cambios se implementan siguiendo los procedimientos operativos estándar en Bitwarden.

Los elementos de Solicitud de Cambio se planifican en base al mapa de ruta y se envían a ingeniería en este punto. La ingeniería revisará y evaluará su capacidad y evaluará el nivel de esfuerzo para cada elemento de solicitud de cambio. Después de revisar y evaluar, formularán en qué van a trabajar para un lanzamiento específico. El CTO proporciona detalles del lanzamiento a través de canales de comunicación y reuniones de gestión y comienza el ciclo de vida de desarrollo para ese lanzamiento.

Desarrollo de alto nivel, proceso de lanzamiento, prueba y aprobación:

- Desarrollando, construyendo e iterando usando solicitudes de extracción en GitHub
- Lleva las funcionalidades a un punto donde sean probables.

- La ingeniería realiza pruebas funcionales de la funcionalidad y/o producto mientras están desarrollando y construyendo.
- La construcción de pruebas unitarias se automatiza como parte de las tuberías de Integración Continua (CI) de Bitwarden.
- Algunas pruebas también son realizadas por el equipo de Éxito del Cliente.
- El Director de Ingeniería ayuda con la revisión y ayuda a formalizar el proceso, incluyendo la actualización de la documentación.
- El CTO proporciona la aprobación final de continuar / no continuar

Asistencia a la reunión: Para garantizar una revisión, aprobación, implementación y cierre exitosos de las solicitudes de cambio, cada miembro del personal central de Operaciones y Servicios de TI debe estar representado durante la reunión para revisar y discutir la solicitud de cambio.

La implementación de emergencia / correcciones urgentes obtienen prioridad elevada, y la revisión y aprobación del cambio se recibe de un gerente o director antes de que se realice el cambio y posteriormente se revisa, se comunica y se cierra durante la próxima reunión programada de cambios. Esto normalmente ocurre en un corte de servicio, sistema caído o en una situación urgente de prevención de interrupciones.

Control de Sistemas de Producción

Bitwarden mantiene libros de ejecución documentados para todos los sistemas de producción, que cubren los procesos de despliegue, actualizar y solución de problemas. Se establecen alertas extensas para notificar y escalar en caso de problemas.

Configuraciones de Línea de Base

Bitwarden procesa y almacena todos los datos de manera segura en la nube de Microsoft Azure utilizando servicios que son gestionados por el equipo de Microsoft. Dado que Bitwarden solo utiliza las ofertas de servicio proporcionadas por Azure, no hay infraestructura de servidor para gestionar y mantener. Todas las actualizaciones y garantías de tiempo de actividad, escalabilidad y seguridad están respaldadas por Microsoft y su infraestructura en la nube.

Las configuraciones del servicio Azure son aprovechadas por Bitwarden para garantizar que las aplicaciones se configuren y se desplieguen de manera repetible y consistente.

Procedimientos de Gestión de Claves de la Plataforma Bitwarden

Las llaves y otros secretos utilizados por la plataforma Bitwarden en sí, incluyen credenciales para las cuentas de los proveedores de la nube de Bitwarden. Todas estas claves se generan, se almacenan de manera segura y se rotan según sea necesario, de acuerdo con las prácticas estándar de la industria. Bitwarden utiliza una caja fuerte interna de Bitwarden para el almacenamiento seguro y la copia de seguridad de claves sensibles u otros secretos utilizados por la plataforma Bitwarden. El control de acceso a la caja fuerte de Bitwarden aprovecha los Tipos de Usuario y Control de Acceso.

Tipos de Datos y Retención de Datos

Bitwarden procesa dos tipos de datos de usuario para proporcionar el Servicio Bitwarden: (i) Datos de la Caja Fuerte y (ii) Datos Administrativos.

(i) Datos de la Caja Fuerte

Los Datos de la caja fuerte incluyen toda la información almacenada dentro de las cuentas del Servicio Bitwarden y pueden incluir Información Personal. Si alojamos el Servicio Bitwarden para usted, alojaremos los Datos de la caja fuerte. Los Datos de la caja fuerte están cifrados utilizando claves criptográficas seguras bajo su control. Bitwarden no puede acceder a los Datos de la caja fuerte.

Retención de Datos de la Caja Fuerte: Puede agregar, modificar y eliminar Datos de la Caja Fuerte en cualquier momento.

(ii) Datos Administrativos

Bitwarden obtiene Información Personal en relación con la creación de su cuenta, el uso del Servicio Bitwarden y el soporte, y los pagos por el Servicio Bitwarden, como nombres, direcciones de correo electrónico, teléfono y otra información de contacto para los usuarios del Servicio Bitwarden y el número de elementos en su cuenta del Servicio Bitwarden ("Datos Administrativos"). Bitwarden utiliza Datos Administrativos para proporcionarte el Servicio de Bitwarden. Retenemos los Datos Administrativos mientras seas un cliente de Bitwarden y según lo requiera la ley. Si termina su relación con Bitwarden, eliminaremos su Información Personal de acuerdo con nuestras políticas de retención de Datos.

Cuando utilice el Sitio o se comunique con nosotros (por ejemplo, a través del correo electrónico), proporcionará y Bitwarden recogerá cierta Información Personal como:

- Nombre
- Nombre de la empresa y dirección
- Número de teléfono de negocios
- Correo electrónico
- Dirección IP y otros identificadores en línea
- Cualquier testimonio de cliente que nos haya dado consentimiento para compartir.
- Información que proporciona a las Áreas Interactivas del Sitio, como formularios rellenables o cuadros de texto, capacitación, seminarios web o registro de eventos.
- Información sobre el dispositivo que está utilizando, que comprende el modelo de hardware, el sistema operativo y la versión, identificadores únicos de dispositivo, información de red, dirección IP y/o información del Servicio Bitwarden cuando interactúa con el Sitio.
- Si interactúas con la Comunidad Bitwarden o con la formación, o te registras para un examen o evento, podemos recopilar información biográfica y el contenido que compartes.
- Información recopilada a través de cookies, etiquetas de píxeles, registros u otras tecnologías similares.

Por favor, consulte la Política de Privacidad de Bitwarden para obtener información adicional.

Registro, Monitoreo y Notificación de Alerta

Bitwarden mantiene libros de ejecución documentados para todos los sistemas de producción que cubren los procesos de despliegue, actualizar y solución de problemas. Se establecen alertas extensas para notificar y escalar en caso de problemas. Una combinación de monitoreo manual y automatizado de la infraestructura en la nube de Bitwarden proporciona una vista completa y detallada de la salud del sistema, así como alertas proactivas en áreas de preocupación. Los problemas se identifican rápidamente para que nuestro equipo de infraestructura pueda responder eficazmente y mitigar los problemas con una mínima interrupción.

Continuidad del Negocio / Recuperación de Desastres

Bitwarden emplea una gama completa de prácticas de recuperación de desastres y continuidad del negocio de Microsoft Azure que están incorporadas en la Nube de Bitwarden. Esto incluye servicios de alta disponibilidad y respaldo para nuestras capas de aplicación y base de datos.

Prevención y Respuesta a Amenazas

Bitwarden realiza evaluaciones de vulnerabilidad de manera regular. Utilizamos herramientas de terceros y servicios externos, incluyendo: OWASP ZAP, Mozilla Observatory, OpenVAS, y otros se utilizan para realizar evaluaciones internas.

Bitwarden utiliza Cloudflare para proporcionar un WAF en el borde, mejor protección DDoS, distribuido disponibilidad y almacenamiento en caché. Bitwarden también utiliza proxies dentro de Cloudflare para una mejor seguridad de red y rendimiento de sus servicios y sitios.

Bitwarden es un software de código abierto. Todo nuestro código fuente está alojado en GitHub y es gratis para que cualquiera lo revise. El código fuente de Bitwarden es auditado por firmas de auditoría de seguridad de terceros de buena reputación, así como por investigadores de seguridad independientes. Además, el Programa de Divulgación de Vulnerabilidades de Bitwarden recluta la ayuda de la comunidad de hackers en HackerOne para hacer Bitwarden más seguro.

Auditoría y Cumplimiento

El Programa de Seguridad y Cumplimiento de Bitwarden se basa en el Sistema de Gestión de Seguridad de la Información (ISMS) ISO27001. Hemos definido políticas que rigen nuestras políticas y procesos de seguridad y continuamente actualizamos nuestro programa de seguridad para ser consistente con los requisitos legales, industriales y regulatorios aplicables para los servicios que proporcionamos bajo nuestro Acuerdo de Términos de Servicio.

Bitwarden cumple con las directrices de seguridad de aplicaciones estándar de la industria que incluyen un equipo de ingeniería de seguridad dedicado y incluyen revisiones regulares del código fuente de la aplicación y la infraestructura de TI para detectar, validar y remediar cualquier vulnerabilidad de seguridad.

Revisiones Externas de Seguridad

Las revisiones y evaluaciones de seguridad de terceros de las aplicaciones y/o la plataforma se realizan como mínimo una vez al año.

Certificaciones

Las certificaciones de Bitwarden incluyen:

- SOC2 Tipo II (renovado anualmente)
- SOC3 (renovado anualmente)

Según la AICPA, el uso del informe SOC 2 Tipo II está restringido. Para consultas sobre el informe SOC 2, por favor contáctenos.

Leer más: Bitwarden logra la certificación SOC2

El informe SOC 3 proporciona un resumen del informe SOC 2 que se puede distribuir públicamente. Según la AICPA, SOC 3 es el informe SOC para las organizaciones de servicios sobre los criterios de servicios de confianza para uso general.
Bitwarden hace una copia de nuestro informe SOC 3 disponible aquí.

Estas certificaciones SOC representan una faceta de nuestro compromiso para salvaguardar la seguridad y la privacidad de los clientes, y el cumplimiento de estándares rigurosos. Bitwarden también realiza una cadencia regular de auditorías en nuestra seguridad de red y la integridad del código de seguridad.

Lea más: La auditoría de seguridad de Bitwarden 2020 está completa y Bitwarden completa la auditoría de seguridad de terceros

Encabezados de Seguridad HTTP

Bitwarden utiliza encabezados de seguridad HTTP como un nivel adicional de protección para la aplicación web de Bitwarden y las comunicaciones. Por ejemplo, HTTP Strict Transport Security (HSTS) obligará a todas las conexiones a usar TLS, lo que mitiga los riesgos de ataques de degradación y mala configuración. Las cabeceras de la Política de Seguridad de Contenido proporcionan una protección adicional contra ataques de inyección, como el scripting entre sitios (XSS). Además, Bitwarden implementa X-Frame-Options: SAMEORIGIN para defenderse contra el clickjacking.

Resumen de Análisis de Modelo de Amenaza y Superficie de Ataque

Bitwarden sigue un enfoque basado en riesgos para diseñar servicios y sistemas seguros que incluyen modelado de amenazas y análisis de superficie de ataque para identificar amenazas y desarrollar mitigaciones para ellas. El análisis de modelado de riesgos y

amenazas se extiende a todas las áreas de la plataforma Bitwarden, incluyendo la aplicación principal del Servidor Cloud de Bitwarden y los Clientes de Bitwarden como Móvil, Escritorio, Aplicación Web, Navegador y/o Interfaz de línea de comandos.

Clientes de Bitwarden

Los usuarios interactúan principalmente con Bitwarden a través de nuestras aplicaciones de cliente como Móvil, Escritorio, Aplicación Web, Navegador y/o Interfaz de línea de comandos. La seguridad de estos dispositivos, estaciones de trabajo y navegadores web es crítica porque si uno o más de estos dispositivos se ven comprometidos, un atacante puede ser capaz de instalar malware como un registrador de teclas que capturaría toda la información ingresada en estos dispositivos, incluyendo cualquiera de tus contraseñas y secretos. Usted, como usuario final y/o propietario del dispositivo, es responsable de garantizar que sus dispositivos estén seguros y protegidos contra el acceso no autorizado.

HTTPS TLS y cifrado de extremo a extremo de criptografía del navegador web

El cliente web de Bitwarden se ejecuta en tu navegador web. La autenticidad e integridad del cliente web de Bitwarden dependen de la integridad de la conexión HTTPS TLS por la cual se entrega. Un atacante capaz de manipular el tráfico que entrega el cliente web podría entregar un cliente malicioso al usuario.

Los ataques a través del navegador web son una de las formas más populares para que los atacantes y ciberdelincuentes inyecten malware o causen daño. Los vectores de ataque en el navegador web podrían incluir:

- Un elemento de **Ingeniería Social, como el Phishing,** para engañar y persuadir a la víctima para que tome cualquier acción que comprometa la seguridad de sus secretos de usuario y cuenta.
- **Ataques al navegador web y extensiones del navegador/exploits complementarios:** una extensión maliciosa diseñada para poder capturar secretos del usuario a medida que se escriben en el teclado.
- **Ataques a aplicaciones web a través del navegador:** Clickjacking, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF).

Bitwarden utiliza Encabezados de seguridad HTTP como un nivel adicional de protección para la aplicación web de Bitwarden y las comunicaciones.

Evaluaciones de Código

Bitwarden es un administrador de contraseñas de código abierto. Todo nuestro código fuente está alojado y disponible públicamente en GitHub para su revisión. El código fuente de Bitwarden ha sido y continúa siendo auditado anualmente por firmas de auditoría de seguridad de terceros de buena reputación, así como por investigadores de seguridad independientes. Además, el Programa de Divulgación de Vulnerabilidades de Bitwarden recluta la ayuda de la comunidad de hackers en HackerOne para hacer Bitwarden más seguro.

Leer más:

- Preguntas frecuentes sobre la seguridad de Bitwarden
- Prevención de Amenazas y Respuesta de Bitwarden
- Evaluaciones de Seguridad y Cumplimiento de Bitwarden, Revisiones, Escaneos de Vulnerabilidad, PenTesting

Conclusión

Esta visión general del programa de Seguridad y Cumplimiento de Bitwarden se ofrece para su revisión. La solución, software, infraestructura y procesos de seguridad de Bitwarden han sido diseñados desde cero con un enfoque de defensa en profundidad y multicapa.

El Programa de Seguridad y Cumplimiento de Bitwarden se basa en el Sistema de Gestión de Seguridad de la Información (ISMS) ISO27001. Definimos políticas que rigen nuestras políticas y procesos de seguridad y continuamente actualizamos nuestro programa

de seguridad para ser consistente con los requisitos legales, industriales y regulatorios aplicables para los servicios que proporcionamos bajo nuestro Acuerdo de Términos de Servicio.

Si tiene alguna pregunta, por favor contáctenos.