PASSWORD MANAGER > BITWARDEN SEND

Enviar Encriptación

Enviar Encriptación

Los envíos son un mecanismo seguro y efímero para transmitir información sensible a cualquiera, incluyendo texto plano y archivos. Como señala el artículo Acerca de Enviar, los Envíos están **cifrados de extremo a extremo**, lo que significa que el cifrado (descrito a continuación) y el descifrado ocurren en el lado del cliente. Cuando creas un Enviar:

1. Se genera una nueva clave secreta de 128 bits para el Enviar.
2. Usando HKDF-SHA256, se deriva una clave de cifrado de 512 bits de la clave secreta.
3. La clave derivada se utiliza para cifrar el envío con AES-256, incluyendo sus datos de archivo/texto y metadatos (nombre, nombre de archivo, notas, y más).

   > **Tip**
   >
   > Cualquier contraseña utilizada para proteger un Enviar **no está involucrada en el cifrado** y descifrado de un Enviar. Las contraseñas son puramente un método de autenticación, sin embargo, los Envíos protegidos por contraseña serán bloqueados para descifrar hasta que la autenticación de la contraseña sea exitosa.

4. El Send cifrado se sube a los servidores de Bitwarden, incluyendo una ID única que Bitwarden usa para identificar el Send para su descifrado pero **sin incluir** la clave de cifrado.

Enviar anatomía

Los envíos se descifran abriendo el enlace Enviar, que se construye a partir de un ID de Enviar único y la clave de cifrado derivada:

```
https://vault.bitwarden.com/#/send_id/clave_de_cifrado
```

Esto tiene varios componentes:

Componente	Ejemplo
Protocolo	https://
Dominio	vault.bitwarden.com
Ancla/fragmento/hash	El ancla/fragmento/hash contiene el id de enviar y la clave de enviar de la URL. En el enlace de ejemplo, esto se representa como `#/send_id/encryption_key`.

El ancla/fragmento/hash no se envía al servidor. Esta información se utiliza localmente dentro del navegador para identificar y descifrar el envío.

Enviar descifrado

Cuando accedes a un enlace Enviar:

1. El navegador web solicita una página de acceso Enviar de los servidores de Bitwarden.
2. Los servidores de Bitwarden devuelven la página de acceso de Enviar como un cliente de caja fuerte web.
3. El cliente de la caja fuerte web analiza localmente el fragmento de URL que contiene la ID de Enviar y la clave de cifrado.
4. El cliente de la caja fuerte web solicita datos del servidor basado en el ID de Enviar analizado. La clave de cifrado **nunca** se incluye en las solicitudes de red.
5. Los servidores de Bitwarden devuelven el Send cifrado al cliente de la caja fuerte web.
6. El cliente de la caja fuerte web descifra localmente el Enviar utilizando la clave de cifrado.

> **Tip**
> Si tu Enviar está protegido por contraseña, el descifrado del Enviar será **bloqueado por autenticación**. El servidor valida la contraseña y solo devuelve el Enviar si la contraseña es correcta. Esto no debe confundirse con la contraseña que se utiliza para el descifrado.

Enviar seguridad

Cuando envías un enlace de Bitwarden Send, hay pasos opcionales que puedes tomar para una seguridad adicional:

1. Agrega una contraseña al Enviar y comparte la contraseña a través de un canal separado.
2. Enviar el enlace sin la clave (todo antes de la última barra inclinada) y enviar la clave a través de un canal separado.
3. Aprovecha ambas opciones anteriores.

> **Tip**
> Al volver a ensamblar una URL de Enviar, asegúrate de incluir tanto el ID de Enviar como la clave de cifrado.
>
> Ejemplo: `https://vault.bitwarden.com/#/enviar/enviar_id/encryption_key`