

PASSWORD MANAGER > COMIENZA

Aplicación Web de Administrador de Contraseñas

Ver en el centro de ayuda:
<https://bitwarden.com/help/getting-started-webvault/>

Aplicación Web de Administrador de Contraseñas

La aplicación web de Bitwarden proporciona la experiencia más rica de Bitwarden para usuarios personales y organizaciones. Muchas funciones importantes, como configurar el [inicio de sesión en dos pasos](#) o administrar una [organización](#), deben realizarse desde la caja fuerte web.

Tip

La aplicación web es accesible desde cualquier navegador web moderno en vault.bitwarden.com y vault.bitwarden.eu. Si estás **autoalojando** Bitwarden, el acceso a la caja fuerte web estará ubicado en tu [dominio configurado](#), por ejemplo <https://my.bitwarden.server.com>.

<input type="checkbox"/>	All	Name	Owner	
<input type="checkbox"/>		Company Credit Card Visa, *4242	My Organiz...	⋮
<input type="checkbox"/>		My Mailing Address Brett Warden	Me	⋮
<input type="checkbox"/>		Personal Login myusername	Me	⋮
<input type="checkbox"/>		Secure Note	Me	⋮
<input type="checkbox"/>		Shared Login username	My Organiz...	⋮

Aplicación web de administrador de contraseñas

Cuando inicies sesión por primera vez en tu aplicación web, aterrizarás en la vista de **Todas las cajas fuertes**. Este espacio enumerará todos los elementos de la caja fuerte, incluyendo [inicios de sesión](#), [tarjetas](#), [identidades](#) y [notas seguras](#).

Primeros pasos

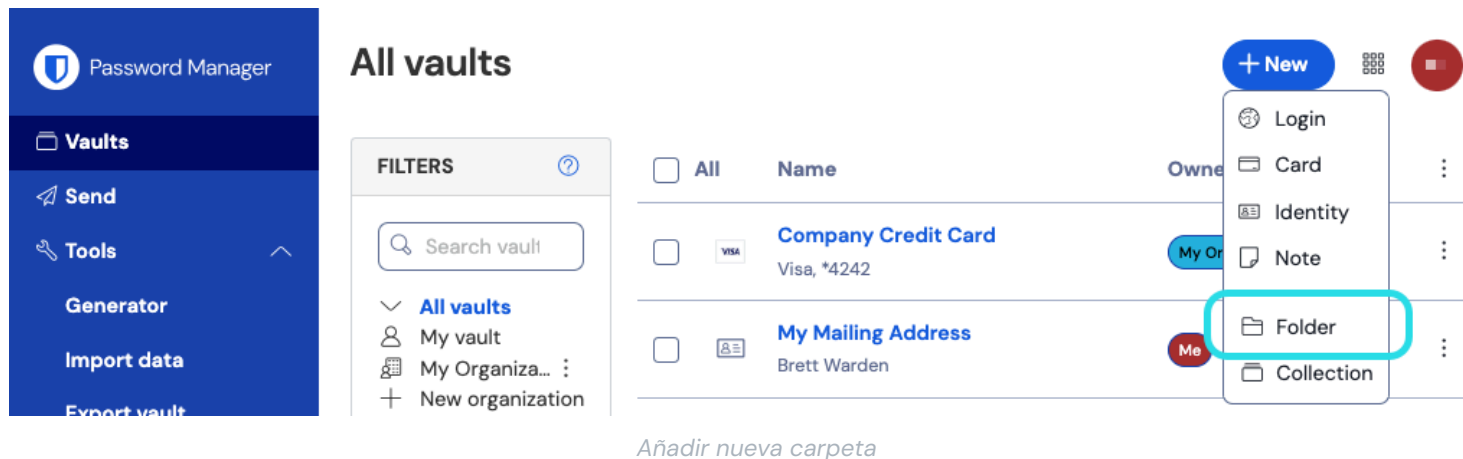
En la captura de pantalla anterior, la vista de **Todas las cajas fuertes** está mostrando **Todos los elementos** en todas las cajas fuertes. Los miembros de [organizaciones](#) tendrán otras bóvedas enumeradas aquí. Usando la columna de **Filtros**, puedes organizar tu caja fuerte en **Favoritos** y **Carpetas**.

Comencemos configurando una nueva carpeta y agregando un nuevo inicio de sesión a ella:

Crea una carpeta

Para crear una carpeta:

1. Seleccione el botón **+ Nuevo** y elija **Carpeta** del menú desplegable:



2. Ingrese un nombre (por ejemplo, **Inicios de sesión en redes sociales**) para su carpeta y seleccione **Guardar**.

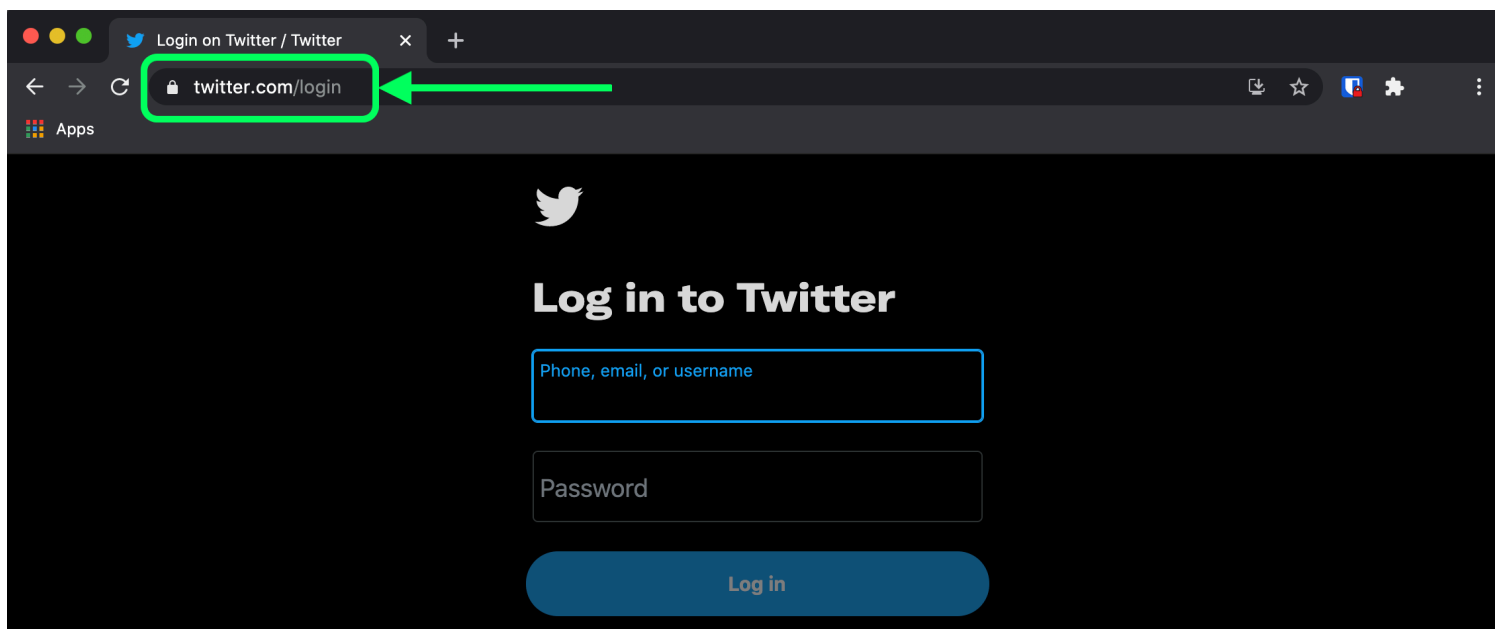
Tip

Para una caja fuerte más limpia, puedes [anidar carpetas dentro de otras carpetas](#).

Añadir un inicio de sesión

Para agregar un nuevo elemento de inicio de sesión:

1. Selecciona el botón **+ Nuevo** y elige **Elemento** del menú desplegable.
2. Seleccione **Inicio de sesión** del menú desplegable (si está agregando una tarjeta, identidad o nota segura en su lugar, seleccione esa opción en su lugar).
3. Ingrese un **Nombre** para el elemento. Los nombres te ayudarán a identificar fácilmente los elementos en tu caja fuerte, así que dale a este elemento un nombre reconocible (por ejemplo, **Mi cuenta de Twitter**).
4. Ingrese su **nombre de usuario** y **contraseña**. Por ahora, ingresa tu contraseña existente. Te ayudaremos a [reemplazarlo con una contraseña más fuerte](#) más tarde.
5. En el campo **URI 1**, ingrese la URL del sitio web (por ejemplo, <https://twitter.com/inicio de sesión>). Si no sabes qué URL usar, navega hasta la pantalla de inicio de sesión del sitio web y cópialo desde tu barra de direcciones.



Encontrando un URI

6. Desde el menú desplegable de **Carpeta**, selecciona el nombre de la carpeta a la que quieres agregar este elemento (por ejemplo, la carpeta de **Inicios de Sesión de Redes Sociales** que creamos anteriormente).

Selecione el icono ☆ **Favorito** para agregar este elemento a tus favoritos. El ícono se llenará (☆ → ★) cuando sea un favorito.

7. ¡Buen trabajo! Seleccione el botón **Guardar** para terminar de agregar este elemento.

Generar una contraseña fuerte

Ahora que un nuevo inicio de sesión está guardado en tu caja fuerte, mejora su seguridad reemplazando la contraseña existente por una más fuerte:

1. En tu caja fuerte, selecciona el elemento que quieres asegurar.
2. En una nueva pestaña o ventana, abre el sitio web correspondiente e inicia sesión en tu cuenta.

💡 Tip

Si ingresaste algo en el campo **URI 1**, haz clic en el icono **Iniciar** para abrirlo directamente desde tu caja fuerte.

3. En ese sitio web, navega hasta el área donde puedes **Cambiar tu contraseña**.

Normalmente, puedes encontrar esto en una sección de **Tu Cuenta**, **Seguridad**, **Ajustes de Inicio de Sesión**, o **Ajustes de Inicio de Sesión**.

4. La mayoría de los sitios web requieren que ingreses tu **contraseña actual** primero. Regresa a tu caja fuerte y selecciona el icono **Copiar** al lado del campo **Contraseña**. Luego, regresa al sitio web y pégalo en el campo **Contraseña actual**.

Es posible que tengas la contraseña antigua memorizada, pero es una buena idea acostumbrarte a copiar y pegar tu contraseña. Así es como iniciarás sesión una vez que tu contraseña sea reemplazada por una más fuerte.

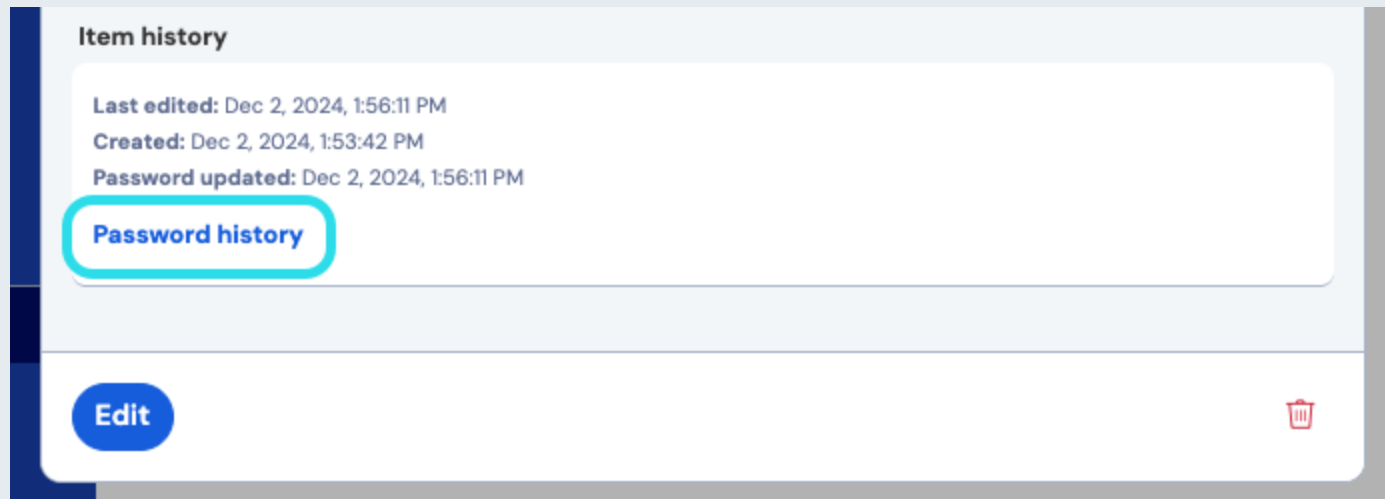
5. Regresa a tu caja fuerte y haz clic en el icono **Generar** al lado del campo **Contraseña**. Se le preguntará si desea sobrescribir la contraseña actual, así que seleccione **Sí** para continuar.

Esto reemplazará tu **Contraseña** con una contraseña fuerte generada aleatoriamente. Pasar de una contraseña como **Fido1234** a **X@Ln@x9J@&u@5n##B** puede detener a un hacker.

6. Copia tu nueva contraseña con el mismo icono  **Copiar** que usaste antes, y selecciona el botón **Guardar**.

Tip

¡No te preocupes por sobrescribir tu contraseña existente! Si algo sale mal, Bitwarden mantiene un **Historial de Contraseñas** de las últimas cinco contraseñas para cada inicio de sesión:



[Ver Historial de Contraseñas](#)

7. Regresa al otro sitio web y pega tu contraseña fuerte en los campos **Nueva Contraseña** y **Confirmar nueva contraseña**.

8. ¡Una vez que **Guardes** el cambio de contraseña, has terminado!

Importa tus datos

¡Buenas noticias! No necesitas repetir este proceso para cada inicio de sesión si tienes nombres de usuario y contraseñas guardados en un navegador web u otro administrador de contraseñas. Utilice una de nuestras guías especializadas de importar para obtener ayuda para transferir sus Datos desde:

- [LastPass](#)
- [1Contraseña](#)
- [Dashlane](#)
- [macOS y Safari](#)
- [Google Chrome](#)
- [Zorro de Fuego](#)

Asegura tu caja fuerte

Ahora que tu caja fuerte está llena de datos, tomemos algunas medidas para protegerla configurando el inicio de sesión en dos pasos. El inicio de sesión en dos pasos requiere que verifiques tu identidad al iniciar sesión utilizando un token adicional, generalmente obtenido de

un dispositivo diferente.

Hay muchos [métodos disponibles](#) para el inicio de sesión en dos pasos, pero el método recomendado para una cuenta gratuita de Bitwarden es usar una aplicación de autenticación de dispositivo móvil como [Authy](#):

1. Descarga Authy en tu dispositivo móvil.

2. En la aplicación web de Bitwarden, selecciona **Ajustes** → **Seguridad** → **Inicio de sesión en dos pasos** desde la navegación:






The screenshot shows the Bitwarden web interface. On the left is a dark blue sidebar with navigation options: Password Manager, Vaults, Send, Tools, Reports, Settings, My account, Security (highlighted), Preferences, Domain rules, Emergency access, Free Bitwarden Famili..., Password Manager, and Admin Console. The main content area is titled 'Security' and has three tabs: 'Master password', 'Two-step login' (selected), and 'Keys'. Below the tabs, the 'Two-step login' section is titled 'Two-step login' and includes a warning box: 'Warning: Setting up two-step login can permanently lock you out of your Bitwarden account. A recovery code allows you to access your account in the event that you can no longer use your normal two-step login provider (example: you lose your device). Bitwarden support will not be able to assist you if you lose access to your account. We recommend you write down or print the recovery code and keep it in a safe place.' A 'View recovery code' button is located below the warning. Underneath is a 'Providers' section with a table of authentication methods:

Provider	Description	Action
Email	Enter a code sent to your email.	Manage
Authenticator app	Enter a code generated by an authenticator app like Bitwarden Authenticator.	Manage
Passkey	Use your device's biometrics or a FIDO2 compatible security key.	Manage
Yubico OTP security key	Use a YubiKey 4, 5 or NEO device.	Manage
Duo	Enter a code generated by Duo Security.	Manage

Autenticación en dos pasos

3. Ubica la opción **Aplicación de Autenticación** y selecciona **Gestionar**:

Providers

	Email Enter a code sent to your email.	Manage
	Authenticator app Enter a code generated by an authenticator app like Bitwarden Authenticator.	Manage
	Passkey Use your device's biometrics or a FIDO2 compatible security key.	Manage
	Yubico OTP security key Use a YubiKey 4, 5 or NEO device.	Manage
	Duo Enter a code generated by Duo Security.	Manage

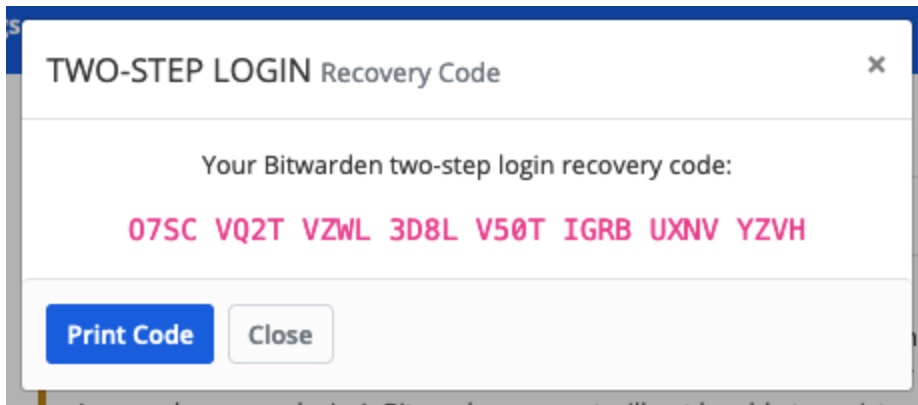
Selecciona el botón Gestionar

Se le pedirá que ingrese su contraseña maestra para continuar.

4. En su dispositivo móvil, abra Authy y toque el botón **+ Agregar Cuenta**.
5. Escanee el código QR ubicado en su caja fuerte web utilizando Authy. Una vez escaneado, Authy mostrará un código de verificación de seis dígitos.
6. Ingrese el código de verificación de seis dígitos en el cuadro de diálogo en su aplicación web y seleccione el botón **Habilitar**.
7. Seleccione el botón **Cerrar** para volver a la pantalla de inicio de sesión de dos pasos, y seleccione el botón **Ver Código de recuperación**.

Tu código de recuperación puede ser utilizado en caso de que pierdas tu dispositivo móvil. **Este es un paso fundamental para garantizar que nunca te quedes fuera de tu bóveda**, ¡así que no te lo saltes!

8. Ingrese su contraseña maestra y seleccione el botón **Continuar** para obtener su Código de recuperación.



Ejemplo de Código de recuperación

Guarda tu código de recuperación de la manera que tenga más sentido para ti. Lo creas o no, imprimir tu código de recuperación y guardarlo en un lugar seguro es una de las mejores formas de asegurarte de que el código no sea vulnerable al robo o a la eliminación inadvertida.

Próximos pasos

¡Felicidades por dominar los conceptos básicos de Bitwarden! Queremos que todos estén seguros en línea, por lo que estamos orgullosos de ofrecer todo lo que has aprendido aquí de forma gratis.

Regístrate para premium

Para usuarios personales, ofrecemos una suscripción Premium por \$10 / año que desbloquea capacidades avanzadas que incluyen:

- Opciones avanzadas de inicio de sesión en dos pasos, como [Duo](#) y [claves de seguridad YubiKey](#)
- Espacio de almacenamiento para [archivos adjuntos cifrados](#)
- Un [Autenticador de Contraseña Única Temporal \(TOTP\)](#) incorporado
- [Acceso de emergencia](#) a su bóveda mediante contactos de emergencia confiables
- [Informes de estado de Vault](#) que informan sobre la seguridad y las contraseñas

Para iniciar una suscripción Premium, selecciona el botón [Ir a Premium](#) desde tu vista de **Cajas Fuertes** !

Inicia una organización

¿Necesita compartir contraseñas u otros elementos de la caja fuerte con sus amigos, Familias, Equipos o toda su empresa?

Las organizaciones de Bitwarden te permiten hacer justamente eso. Recomendamos probar la funcionalidad de compartir contraseñas de las organizaciones al [iniciar una organización gratuita para dos personas](#).

Una vez que hayas probado una organización, visita nuestra página de [precios de Bitwarden](#) para aprender sobre los diferentes tipos de organización que podrías considerar.