

ADMINISTRADOR DE SECRETOS > COMIENZA

Inicia sesión en el Administrador de secretos

Ver en el centro de ayuda:

<https://bitwarden.com/help/log-in-to-secrets-manager/>

Inicia sesión en el Administrador de secretos

La cuenta de Bitwarden cifrada de extremo a extremo con conocimiento cero que utilizas para iniciar sesión en el administrador de contraseñas será la misma que utilizas para iniciar sesión en el Administrador de secretos.

Tip

Este artículo se refiere a iniciar sesión en la caja fuerte web del Administrador de secretos. El ILC del [Administrador de secretos](#), que se utiliza principalmente para gestionar la inyección de secretos en sus aplicaciones e infraestructura, requiere [iniciar sesión con un token de acceso](#).

Contraseña maestra

Tu contraseña maestra es el método principal para acceder a tu cuenta de Bitwarden. Es importante que tu contraseña maestra sea:

- **Memorable** : los empleados y sistemas de Bitwarden no tienen conocimiento ni forma de recuperar ni de restablecer su contraseña maestra. **¡No olvides tu contraseña maestra!**
- **Fuerte** : una contraseña maestra más larga, más compleja y menos común es la mejor manera de proteger su cuenta. Bitwarden proporciona una herramienta de prueba de fuerza de contraseña gratis para probar la fuerza de algunas contraseñas memorables que estás considerando.

Tip

¿Preocupado por olvidar tu contraseña maestra? Aquí está lo que hay que hacer:

- **Configura una pista.** En caso de que necesites un recordatorio, se puede solicitar un correo electrónico con una pista para la contraseña maestra en la pantalla de inicio de sesión. Asegúrate de usar una pista que solo tú entenderás.
- **Designa un contacto de emergencia de confianza.** Los usuarios con acceso Premium pueden otorgar acceso a la cuenta a un amigo o familiar en caso de emergencia.

Aprende cómo [cambiar tu contraseña maestra](#), o qué hacer si has [olvidado tu contraseña maestra](#).

Autenticación en dos pasos

Usar el [inicio de sesión en dos pasos](#) (también llamado autenticación de dos factores o 2FA) para proteger tu cuenta de Bitwarden evita que un actor malintencionado acceda a tus datos incluso si descubren tu contraseña maestra al requerir autenticación desde un dispositivo secundario cuando inicias sesión.

Hay muchos métodos diferentes para el inicio de sesión en dos pasos, que van desde aplicaciones dedicadas de autenticación hasta claves de seguridad de hardware. Lo que elijas, Bitwarden recomienda encarecidamente que asegures tu caja fuerte utilizando inicio de sesión de dos pasos.

Métodos gratis

Bitwarden ofrece varios métodos de inicio de sesión en dos pasos gratis, incluyendo:

Método	Instrucciones de configuración
a través de una aplicación de autenticación (por ejemplo, Authy o Google Authenticator)	Haz clic aquí .
vía correo electrónico	Haz clic aquí .
a través de un Autenticador WebAuthn FIDO	Haz clic aquí .

Métodos premium

Para los usuarios Premium (incluyendo miembros de organizaciones pagadas), Bitwarden ofrece varios métodos avanzados de inicio de sesión en dos pasos:

Método	Instrucciones de configuración
a través de Duo Security con Duo Push, SMS, llamada telefónica y claves de seguridad	Haz clic aquí .
vía YubiKey (cualquier dispositivo de la serie 4/5 o YubiKey NEO/NFC)	Haz clic aquí .

Iniciar sesión con el dispositivo

¿Sabías que puedes iniciar sesión en la aplicación web de Bitwarden usando un dispositivo secundario en lugar de tu contraseña maestra? Iniciar sesión con un dispositivo es un enfoque de autenticación sin contraseña, eliminando la necesidad de ingresar su contraseña maestra al enviar solicitudes de autenticación a cualquier dispositivo específico en el que actualmente haya iniciado sesión para su aprobación. [Más información](#).

Inicio de sesión único

Si su organización utiliza [inicio de sesión con SSO](#), puede acceder a su aplicación web Bitwarden [usando sus credenciales federadas de SSO](#).