

VAULTWARDEN

FUNCIONAMIENTO

19-03-2025

Tabla de contenido

¿Que es vaultwarden?	3
Registro y acceso:	3
Contrasenas:	7
Organizaciones:	9
Configuración de navegador	17

¿Qué es Vaultwarden?

En gestor de contraseñas seguro).

En pocas palabras:

Guarda todas tus contraseñas en un solo lugar, cifradas y protegidas.

Sincroniza tus claves entre dispositivos (PC, móvil, tablet).

Genera contraseñas fuertes automáticamente.

Para la empresa: Lo controla el equipo de TI, reduciendo riesgos de fugas.

Ventaja para empleados:

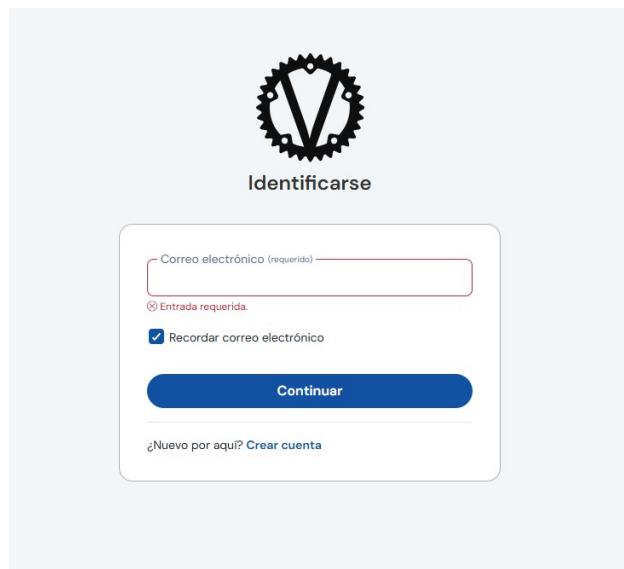
Más seguro que anotar contraseñas en post-its o documentos.

Fácil de usar: Acceso rápido sin recordar decenas de claves.

"Como una caja fuerte digital para tus contraseñas, pero más simple y controlada por la empresa."

Registro y acceso:

- **Crear una cuenta:** Accede a la interfaz web de Vaultwarden a través de tu navegador (<https://passwords.mtda.es/>)



Aquí le daremos a crear una cuenta para registrarnos

Crear cuenta

Correo electrónico (requerido) _____
Utilizarás tu correo electrónico para acceder.

Nombre _____

¿Cómo deberíamos llamarle?

Contraseña maestra (requerido) _____ 

Importante: ¡Las contraseñas maestras no pueden ser recuperadas si las olvidas! 12 caracteres mínimo

Vuelve a escribir tu contraseña maestra (requerido) _____ 

Pista de contraseña maestra _____
Una pista de tu contraseña maestra puede ayudarte a recordarla en caso de que la olvides.

Comprobar filtración de datos conocidas para esta contraseña

Crear cuenta

¿Ya tienes una cuenta? [Identificarse](#)

Introducimos los datos solicitados; ponemos el correo el nombre y la contraseña maestra; muy importante no olvidar de colocar una pista de la contraseña ya que esta será la que nos permitirá luego recuperar la contraseña.

- **Iniciar sesión:** Despues de crear tu cuenta, utiliza tus credenciales para acceder a la bóveda de contraseñas.

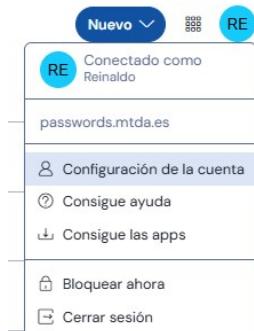
Una vez iniciado sesión nos aparecerá esta pantalla que será como el panel personal de cada usuario y aquí podremos ya gestionar el contenido que vamos a almacenar.

En el contenido para almacenar tenemos varias opciones: inicio de sesión, datos de tarjetas, identidad y notas seguras; la parte que más nos interesa es la de inicio de sesión

- Doble factor:

Para reforzar la seguridad de la cuenta, se recomienda habilitar el factor de doble autenticación (2FA).

Para ello, es necesario acceder al menú de usuario, ubicado en la esquina superior derecha, y seleccionar la opción "**Configuración de la cuenta**".



Una vez dentro de **Configuración de la cuenta**, en el panel lateral izquierdo, accedemos al apartado **Seguridad**. En esta sección, debemos seleccionar la pestaña "**Autenticación en dos pasos**".

Desde allí podremos iniciar el proceso de configuración del segundo factor de autenticación

The screenshot shows the Vaultwarden Password Manager interface. On the left is a dark sidebar with navigation links: Cajas fuertes, Enviar, Herramientas, Informes, Configuración (which is currently selected), Mi cuenta, Seguridad, Preferencias, Reglas de dominios, and Acceso de emergencia. The main content area has a light background and a header "Seguridad". Below the header are tabs: Contraseña maestra (disabled), Autenticación en dos pasos (selected), Devices, and Claves. Under the "Autenticación en dos pasos" tab, there's a section titled "Advertencia" with a warning about enabling 2FA. A button "Ver código de recuperación" is visible. Below this is a section titled "Proveedores" listing various 2FA methods: Correo electrónico, Aplicación de autenticación (with a checkmark), FIDO2 WebAuthn, yubico, and DUO. Each method has a small icon, a brief description, and a "Gestionar" button.

Una vez en el apartado **Autenticación en dos pasos**, se podrá elegir el método de verificación preferido:

Correo electrónico: el sistema enviará un código temporal al correo asociado a la cuenta. Dicho código deberá ser ingresado para completar el proceso de activación.

Aplicación de autenticación: se mostrará un código QR que deberá ser escaneado con una aplicación compatible (como Google Authenticator, Authy, etc.). La app generará un código temporal que deberá introducirse para validar y completar la configuración.

Ambos métodos proporcionan una capa adicional de seguridad al requerir un segundo factor además de la contraseña habitual.

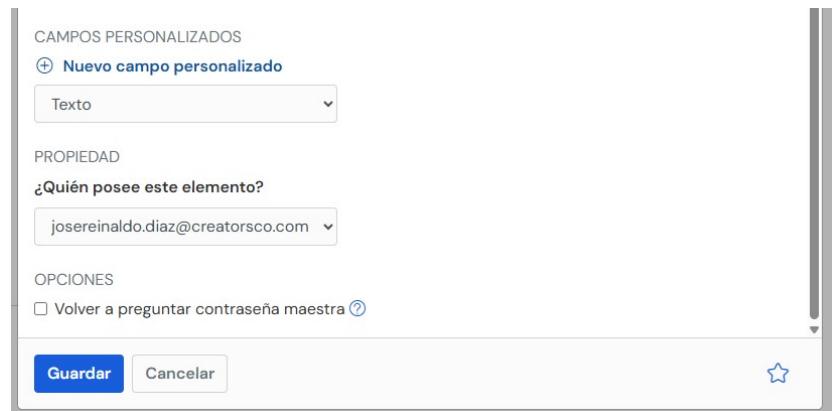
Contraseñas:

Para guardar contraseñas estas las podemos guardar en carpetas o en colecciones o directamente crearlas sin un directorio específico, en vaultwarden las contraseñas son tratadas con el nombre de elementos, y para crear uno nuevo nos iremos a la esquina superior derecha y daremos a nuevo -> elemento



The screenshot shows the "NUEVO ELEMENTO" (New Element) dialog box. It has the following fields and features:

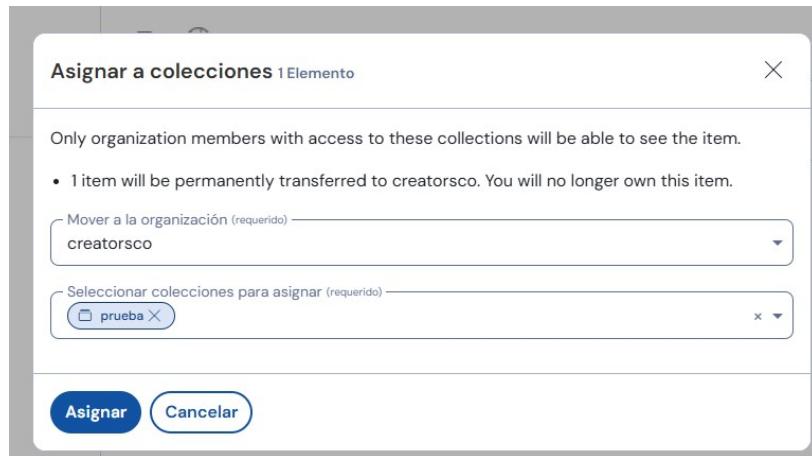
- ¿Qué tipo de elemento es este?**: A dropdown menu currently set to "Inicio de sesión".
- Nombre**: An input field for the element name.
- Carpeta**: A dropdown menu for selecting a folder.
- Usuario**: An input field for the user account.
- Contraseña**: An input field for the password, with icons for copy, clear, and eye.
- Clave de autenticación (TOTP)**: An input field for TOTP authentication code, with a placeholder "15" and a copy icon.
- URI 1**: An input field with placeholder "ej. https://google.com" and a copy icon.
- Tipo de detección**: A dropdown menu currently set to "Detección por defecto".
- + Nueva URI**: A button to add more URIs.
- Notas**: A text area for notes.
- CAMPOS PERSONALIZADOS**: A section at the bottom with "Guardar" (Save) and "Cancelar" (Cancel) buttons, and a star icon.



Una vez aquí ya nos sale para llenar los datos de las credenciales y la configuración de autenticación de la misma así como el dueño de la contraseña.

Una vez almacenada para compartirlo lo que habrá que hacer es dar clic sobre los tres puntos y darle a añadir a colección y allí seleccionamos la colección dentro de la organización a la que se compartirá la contraseña.

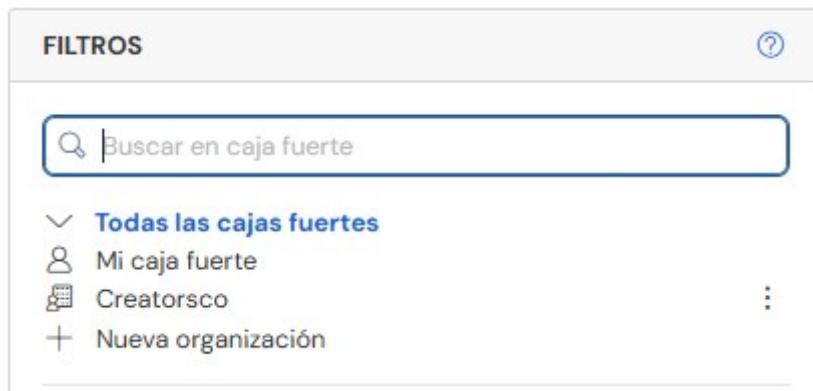
- Copiar usuario
- Copiar contraseña
- Iniciar
- Adjuntos
- Clonar
- Asignar a colecciones
- Eliminar



Y con esto ya estaría compartida la contraseña para todos los

usuarios de la organización que tienen acceso a esa colección.

Una vez almacenadas las credenciales tanto en el espacio de la organización como en el repositorio personal, su diferenciación puede realizarse mediante el panel lateral izquierdo, específicamente en la sección "Filtros", donde se puede seleccionar la fuente de origen de cada elemento.



En el panel lateral, dentro del apartado "Filtros", se presentan las siguientes opciones de visualización:

- **Todas las cajas fuertes:** Muestra de forma consolidada todas las credenciales a las que el usuario tiene acceso, incluyendo tanto las personales como las compartidas por la organización.
- **Mi caja fuerte:** Filtra exclusivamente las credenciales privadas del usuario, es decir, aquellas que no han sido compartidas ni forman parte de una organización.
- **Creatorsco:** Corresponde a la bóveda de la organización. Aquí se muestran únicamente las credenciales a las que el usuario tiene acceso. Si no se poseen permisos sobre determinados elementos compartidos por la organización, estos no serán visibles.

Organizaciones:

En Vaultwarden, las organizaciones funcionan como grupos de usuarios que permiten la gestión colaborativa de contraseñas. A cada organización se le pueden asignar colecciones, que actúan como carpetas organizadas donde se almacenan las contraseñas, facilitando el acceso compartido y seguro entre los miembros.

Para crear una organización lo que debemos hacer es lo siguiente:

Primero que nada esto lo haremos con el usuario que sera admin de la administración; luego vamos a todas las cajas fuertes, y damos a "nueva organización"

The screenshot shows the Vaultwarden Password Manager interface. On the left is a dark sidebar with white text and icons: 'Cajas fuertes', 'Enviar', 'Herramientas', 'Informes', and 'Configuración'. The main area has a title 'Todas las cajas fuertes'. Below it is a 'FILTROS' section with a search bar 'Buscar en caja fuerte'. A dropdown menu lists 'Todas las cajas fuertes', 'Mi caja fuerte', 'creatorsco', 'SISTEMAS', and '+ Nueva organización', with the last option circled in blue.

Y seguido de esto ya nos pediría el nombre de la organización y el correo que la administra

Nueva organización

Las organizaciones te permiten compartir partes de tu caja fuerte con otras personas así como gestionar que usuarios están relacionado con una entidad concreta como familia, un pequeño equipo o una gran empresa.

Información general

Nombre de la organización (requerido) _____ Correo electrónico (requerido) _____

josereinaldo.diaz@creatorsco.com

Enviar

Una vez creada la organización se nos habilita ya la consola de admin donde podremos gestionar todas las configuraciones de lo que seria la organización

Algunas de las cosas que podemos mirar desde este panel son las siguientes:

Informes

Identifique y cierre las lagunas de seguridad en las cuentas de su organización haciendo clic en los siguientes informes.

Informe de contraseñas comprometidas Las contraseñas comprometidas en una brecha de datos son blancos fáciles para los atacantes. Cambia estas contraseñas para evitar futuras intrusiones.	Contraseñas reutilizadas Si un servicio que usa está comprometido, reutilizar la misma contraseña en otros lugares puede permitir que los hackers accedan fácilmente a más de sus cuentas en línea. Debe utilizar una contraseña única para cada cuenta o servicio.	Contraseñas débiles Contraseñas débiles pueden ser fácilmente adivinadas por hackers y herramientas automatizadas que se utilizan para descifrar contraseñas. El generador de contraseñas de Bitwarden puede ayudarle a crear contraseñas fuertes.
Informes de sitios web no seguros Usar sitios web no seguros con el esquema <code>http://</code> puede ser peligroso. Si el sitio web lo permite, se debe acceder siempre usando el esquema <code>https://</code> para que la conexión esté cifrada.	Informe 2FA inactivo La autenticación de dos factores (2FA) es una configuración de seguridad importante que ayuda a proteger sus cuentas. Si el sitio web lo ofrece, siempre debe habilitar la autenticación de dos factores.	

Información de la organización

Nombre de la organización (requerido)	<input type="text" value="creatorsco"/>	
Correo electrónico (requerido)	<input type="text" value="josereinaldo.diaz@creatorsco.com"/>	
<small>Frase de la huella digital de su organización: <code>umolded-crudely-sequence-opal-alive</code></small>		
Guardar		

Clave API

Su clave API puede ser usada para autenticar la API pública de Bitwarden. [Learn more about Bitwarden's API](#)

[Ver clave API](#) [Regenerar clave API](#)

Zona peligrosa

¡Cuidado, estas acciones no son reversibles!	
Eliminar organización	Caja fuerte purgada

Políticas

Requiere inicio de sesión en dos pasos

Requiere que los usuarios establezcan un inicio de sesión en dos pasos en sus cuentas personales.

Requisitos de la contraseña maestra

Establecer requisitos mínimos para la fortaleza de la contraseña maestra.

Administración de recuperación de cuenta

Basándose en el método de cifrado, recupera las cuentas cuando se olviden o pierdan las contraseñas maestras o los dispositivos de confianza.

Generador de contraseñas

Establecer requisitos mínimos para la configuración del generador de contraseñas.

Organización única

Restringir a los usuarios de ser capaces de unirse a otras organizaciones.

Propiedad personal

Requiere que los usuarios guarden los elementos de la caja fuerte en una organización por eliminando la opción de propiedad personal.

Desactivar envío

No permitir a los usuarios crear o editar un Send de Bitwarden. Eliminar un Send existente todavía está permitido.

Opciones del Send

Establecer opciones para crear y editar los Send.

Importar datos

Destination

Colección —

-- Seleccione una colección --

Seleccione esta opción si desea que el contenido del archivo importado se traslade a un colección

Data

Formato de archivo (requerido) —

-- Selecciona --

Seleccionar el fichero a importar —

Seleccionar archivo No se ha seleccionado ningún archivo

o copia/pega el contenido del fichero a importar —

Importar datos

Exportar caja fuerte

ⓘ Exportando caja fuerte de la organización

Only the organization vault associated with creatorsco will be exported. Items in individual vaults or other organizations will not be included.

Exportar desde (requerido) —

creatorsco

Formato de archivo (requerido) —

.json

Confirmar formato

Con esto, ya tendríamos configurada la estructura básica de la organización. Ahora pasemos a la gestión de usuarios.

Una vez creada la organización, en el **panel de administración** encontraremos una sección llamada "**Miembros**". Desde allí, podemos invitar usuarios para que formen parte de la organización, asignarles roles específicos (como administrador, gestor o usuario) y controlar los permisos que tendrán sobre las diferentes colecciones compartidas. Esto permite definir quién puede acceder, modificar o simplemente visualizar las contraseñas dentro de la organización

The screenshot shows the 'Miembros' (Members) section of the Vaultwarden Admin Console. On the left is a sidebar with navigation links: 'creatorsco' (selected), 'Colecciones', 'Miembros' (selected), 'Informes', and 'Configuración'. The main area has a header with a search bar ('Buscar miembros'), a '+ Invitar miembro' button, and a 'RE' button. Below the header is a filter bar with tabs: 'Todo' (4), 'Invitado' (1), 'Necesita confirmación', and 'Revocado'. A table lists five users:

	Nombre	Colecciones	Rol	Políticas	⋮
<input type="checkbox"/>	adrian.aparicio@creatorsco.com (Invitado)		Usuario		⋮
<input type="checkbox"/>	Carla carla.alvarez@creatorsco.com	(Colección por defecto) prueba	Usuario		⋮
<input type="checkbox"/>	Iván ivan.juliana@creatorsco.com	(Colección por defecto) prueba	Usuario		⋮
<input type="checkbox"/>	reinaldo josereinaldo.diaz@creatorsco.com		Propietario		⋮

En esta sección se muestran los miembros actuales de la organización, junto con los usuarios invitados, aquellos que aún no han confirmado su invitación y los usuarios revocados.

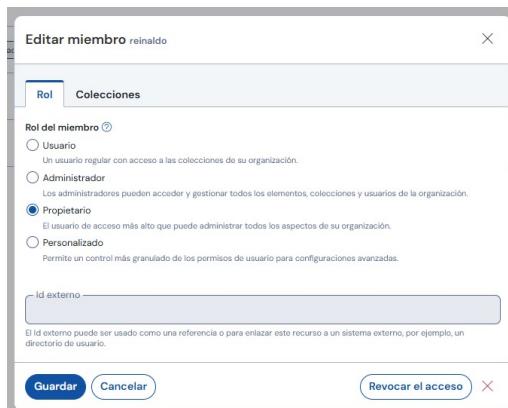
Desde este panel, podemos gestionar cada usuario de manera individual, asignándoles permisos y roles específicos (como administrador, gestor o miembro estándar). Además, podemos controlar a qué colecciones tendrá acceso cada uno, garantizando que solo vean las contraseñas y datos que realmente necesitan según su función dentro de la organización.

Para editar un usuario, simplemente hacemos clic en su nombre, lo que abrirá una nueva ventana con sus opciones de configuración.

En esta ventana, podemos asignarle un rol específico. Las opciones disponibles son:

- **Propietario:** Tiene control total sobre la organización, incluyendo la gestión de usuarios, colecciones y configuración general.
- **Administrador:** Puede gestionar miembros y colecciones, pero no tiene el mismo nivel de control que el propietario.
- **Usuario:** Solo puede acceder a las colecciones que se le asignen, sin permisos de administración.
- **Personalizado:** Permite definir permisos a medida, ajustando qué acciones puede realizar el usuario dentro de la organización.

Esta flexibilidad ayuda a mantener la seguridad y el orden, permitiendo que cada miembro tenga solo el nivel de acceso que necesita.



En la pestaña de **Colecciones**, podemos definir los permisos de cada usuario sobre las colecciones específicas a las que tendrá acceso. Los permisos disponibles son:

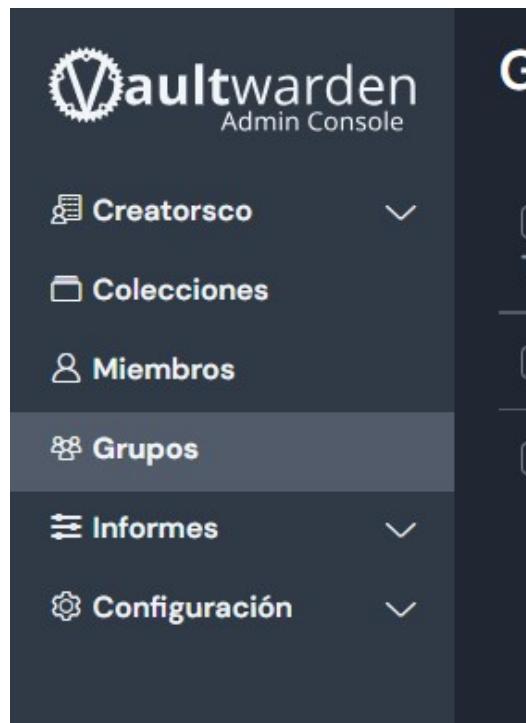
- **Puede ver:** El usuario tiene acceso para ver todos los elementos de la colección, incluidas las contraseñas.
- **Puede ver, excepto contraseñas:** El usuario puede ver los elementos, pero las contraseñas estarán ocultas.

- **Puede editar:** El usuario puede modificar los elementos dentro de la colección, pero no puede gestionar los permisos de otros usuarios.
- **Puede editar, excepto contraseñas:** Permite al usuario editar todos los elementos de la colección, excepto las contraseñas.
- **Puede gestionar:** El usuario tiene control total sobre la colección, incluyendo la capacidad de agregar, editar, eliminar elementos y gestionar los permisos de otros usuarios dentro de esa colección.

Una vez establecidos los permisos, simplemente se aplican a cada colección a la que el usuario tenga acceso el permiso específico, garantizando que cada miembro tenga el nivel de acceso adecuado.

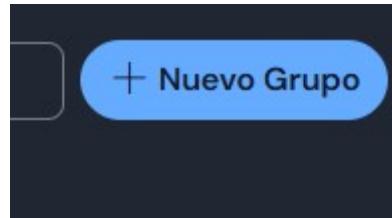


Por otro lado, también podemos crear **grupos**. Una vez que los usuarios estén creados, encontraremos la sección de **Grupos** debajo del apartado de **Miembros**.



Aquí podremos configurar los distintos grupos de la empresa y asignar a cada usuario a su grupo correspondiente.

Para crear un nuevo grupo, el proceso es similar al de añadir una colección. Lo primero que debemos hacer es hacer clic en el botón que dice "**Nuevo grupo**".



En la ventana emergente, deberemos completar la siguiente información:

- **Nombre del grupo:** Asignamos un nombre que identifique al grupo.
- **Miembros:** Seleccionamos los usuarios que formarán parte de este grupo.
- **Colecciones:** Elegimos las colecciones a las que el grupo tendrá acceso y configuraremos los permisos correspondientes.

Una vez completados estos datos, el grupo quedará configurado y listo para usarse.

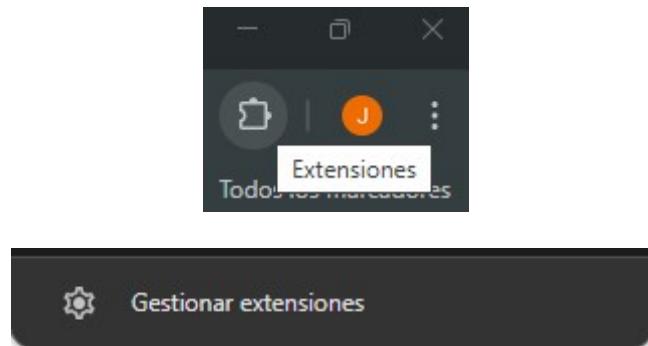
The image displays three separate screenshots of the Bitwarden 'Nuevo Grupo' (New Group) dialog box, each showing a different tab: 'Información del grupo', 'Miembros', and 'Colecciones'.

- Información del grupo:** This tab shows fields for 'Nombre (requerido)' (Name required) and 'Id externo'. A note states: 'El Id externo puede ser usado como una referencia o para enlazar este recurso a un sistema externo, por ejemplo, un directorio de usuario.' (The external ID can be used as a reference or to link this resource to an external system, such as a user directory). Buttons for 'Guardar' (Save) and 'Cancelar' (Cancel) are at the bottom.
- Miembros:** This tab is titled 'Nuevo Grupo' and shows a section for 'Otorgar a los miembros acceso a las colecciones asignadas por el grupo.' (Grant members access to the collections assigned by the group). It includes a dropdown for 'Seleccionar miembros' (Select members) and a note: '-- Escriba para filtrar --'. Below is a table with columns 'Miembro' (Member) and 'Rol' (Role), showing 'Ningún miembro añadido' (No members added). Buttons for 'Guardar' (Save) and 'Cancelar' (Cancel) are at the bottom.
- Colecciones:** This tab is also titled 'Nuevo Grupo' and shows a section for 'Conceder acceso a las colecciones añadiéndolas a este grupo.' (Grant access to collections by adding them to this group). It includes a dropdown for 'Permiso' (Permission) set to 'Puede ver' (Can view) and a dropdown for 'Seleccionar colecciones' (Select collections) with the note: '-- Escriba para filtrar --'. Below is a table with columns 'Colección' (Collection) and 'Permiso' (Permission), showing 'No hay colecciones añadidas' (No collections added). Buttons for 'Guardar' (Save) and 'Cancelar' (Cancel) are at the bottom.

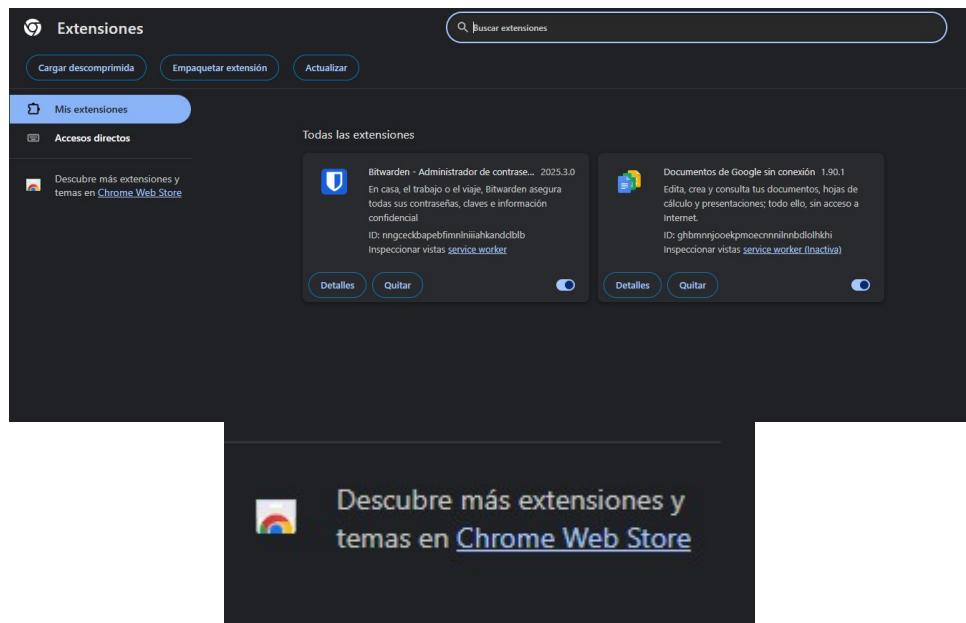
Configuración de navegador

A continuación, debemos proceder con la configuración de la extensión de Bitwarden en el navegador. Esto nos permitirá utilizar nuestro gestor de contraseñas y que este se encargue de completar automáticamente las credenciales en los distintos sitios web.

Para comenzar, lo primero que debemos hacer es dirigirnos al ícono de extensiones en el navegador, el cual tiene la forma de una pieza de rompecabezas, y le damos a gestionar extensiones



Al hacer clic en el ícono de extensiones, se abrirá una ventana en la que podremos ver las extensiones instaladas en nuestro navegador. En mi caso, la extensión de Bitwarden ya aparece porque la he configurado previamente; sin embargo, es probable que no aparezca en el suyo. Para instalarla, deben hacer clic en el enlace que dice "Descubre más extensiones" y acceder al siguiente enlace proporcionado.



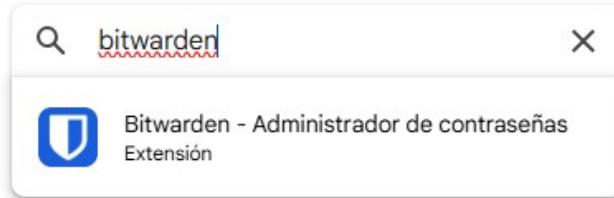
The screenshot shows the Bitwarden Extension Manager interface. At the top, there are buttons for 'Cargar descomprimida' (Unzip), 'Empaquetar extensión' (Pack extension), and 'Actualizar' (Update). Below this, a sidebar has 'Mis extensiones' selected. A central area shows 'Todas las extensiones' with two extensions listed:

- Bitwarden - Administrador de contraseñas** (2025.3.0)
Descripción: En casa, el trabajo o el viaje, Bitwarden asegura todas sus contraseñas, claves e información confidencial.
ID: nngceckkapebfimnnihahandclbb
Inspeccionar vistas *service worker*
[Detalles](#) [Quitar](#)
- Documentos de Google sin conexión** (1.90.1)
Descripción: Edita, crea y consulta tus documentos, hojas de cálculo y presentaciones; todo ello, sin acceso a Internet.
ID: gbnmnyyookpmoeonninnbdolhkh
Inspeccionar vistas *service worker (inactiva)*
[Detalles](#) [Quitar](#)

At the bottom left, there is a call-to-action button with the text 'Descubre más extensiones y temas en [Chrome Web Store](#)'.

https://chromewebstore.google.com/category/extensions?utm_source=ext_sidebar&hl=en

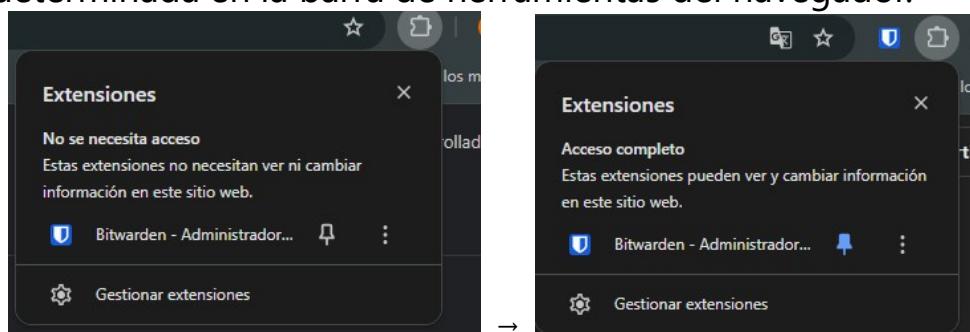
Una vez que abrimos el enlace, debemos utilizar el buscador de la tienda de extensiones e ingresar el nombre de la extensión: "Bitwarden".



A continuación, seleccionamos la extensión de Bitwarden y hacemos clic en el botón de "Instalar" para añadirla a nuestro navegador.



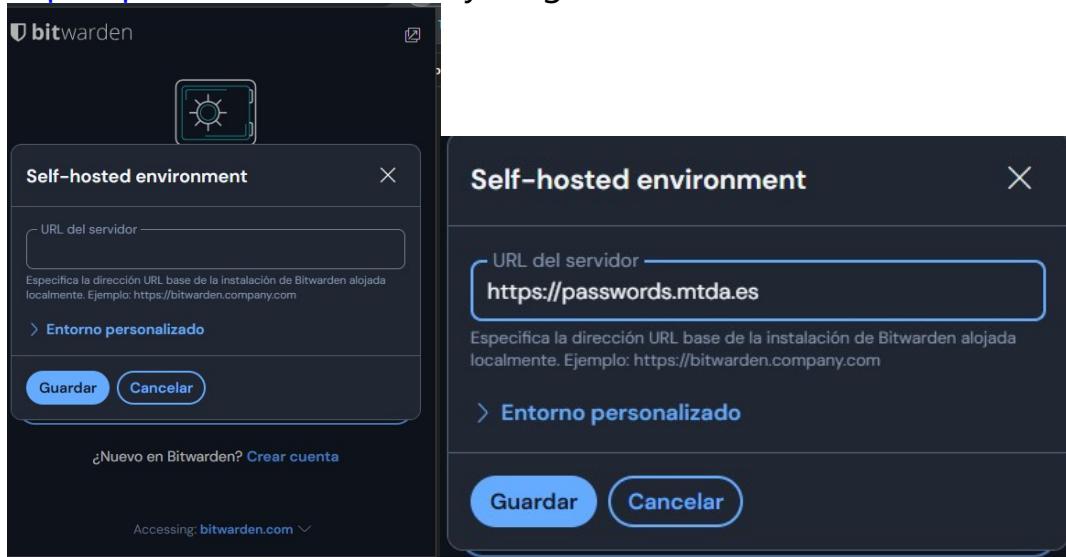
Una vez que la extensión esté instalada, volvemos a hacer clic en el ícono de las extensiones en el navegador. Ahora debería aparecer la extensión de Bitwarden. Para facilitar su acceso, hacemos clic en el ícono del alfiler para que la extensión se muestre de manera predeterminada en la barra de herramientas del navegador.



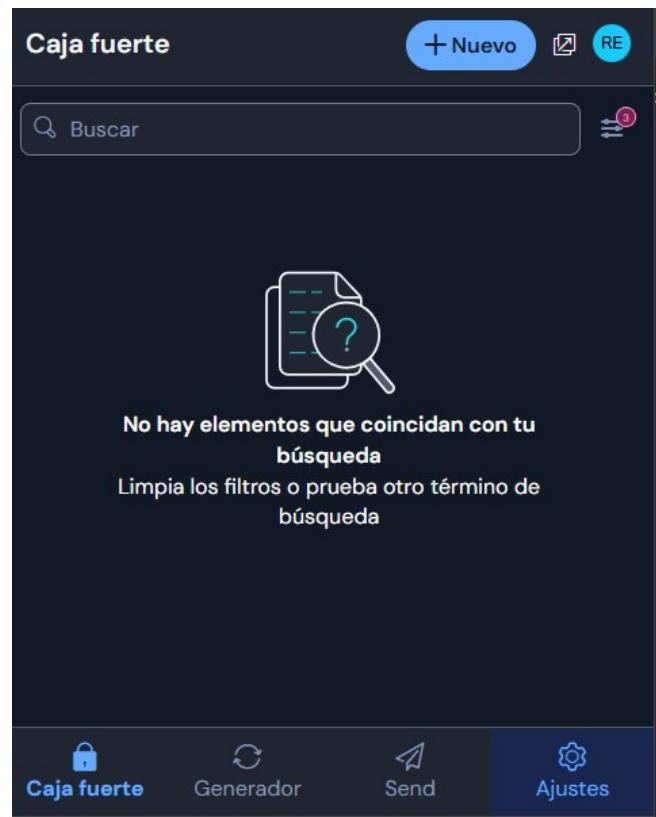
Con esto completado, abrimos la extensión y lo primero que debemos hacer es dirigirnos a la parte inferior, donde aparece la opción "Accessing". Allí, cambiamos la configuración de "Bitwarden" a "Autoalojado".



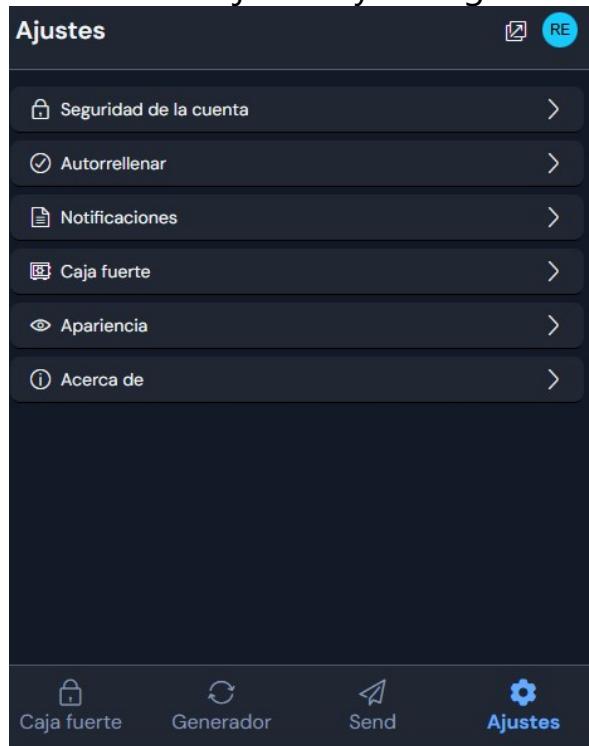
Al seleccionar la opción "Autoalojado", se nos pedirá la URL del servidor. Debemos copiar y pegar la siguiente dirección: "<https://passwords.mtda.es>" y luego hacer clic en "Guardar".



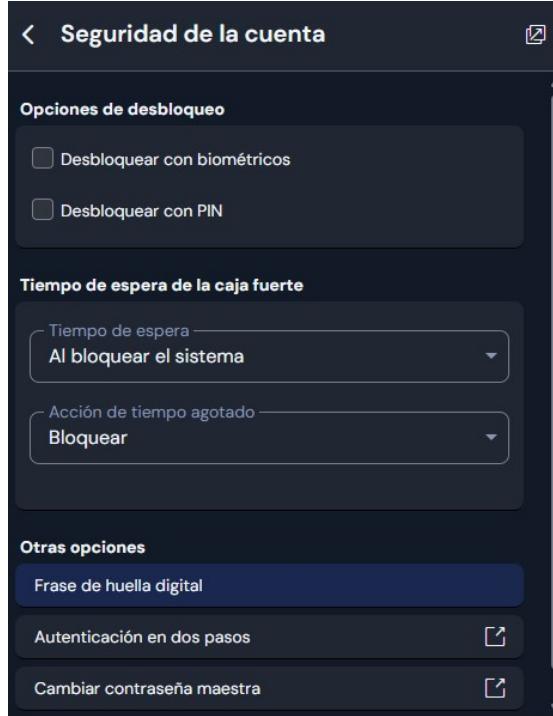
De esta manera, el diseño de la interfaz cambiará ligeramente. Lo único que nos quedará por hacer es acceder a nuestra cuenta utilizando nuestro correo electrónico y contraseña. Una vez hecho esto, nuestras credenciales deberían aparecer automáticamente en la extensión.



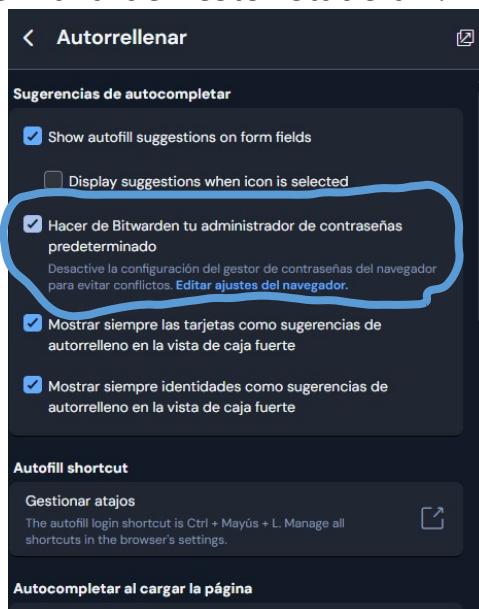
Una vez que hemos accedido, lo único que nos queda es realizar una pequeña configuración dentro de la extensión. Para ello, debemos ir a la sección de "Ajustes" y configurar lo siguiente:

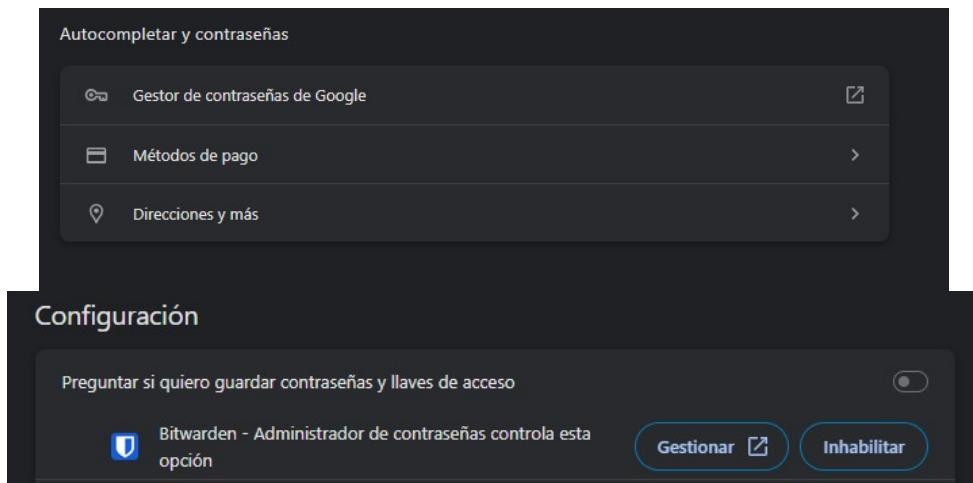


1. Seguridad de la cuenta: En esta sección, estableceremos el tiempo de espera de la aplicación. Configuramos este valor de la siguiente manera:



2. Autorellenar: En esta sección, debemos habilitar la casilla marcada. Luego, procedemos a hacer clic en "Editar ajustes del navegador" → "Gestor de contraseñas" → "Configuración" y verificamos que Bitwarden esté listado allí.





Con esto, ya tendríamos la extensión configurada en el navegador. Para utilizarla, simplemente debemos hacer clic en el ícono de Vaultwarden (el escudo azul y blanco) cuando necesitemos introducir una credencial. Luego, seleccionamos las credenciales que deseamos utilizar y la extensión las rellenará automáticamente, permitiéndonos acceder sin ningún problema.