VAULTWARDEN

FUNCIONAMIENTO

19-03-2025

Tabla de contenido

¿Que 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.

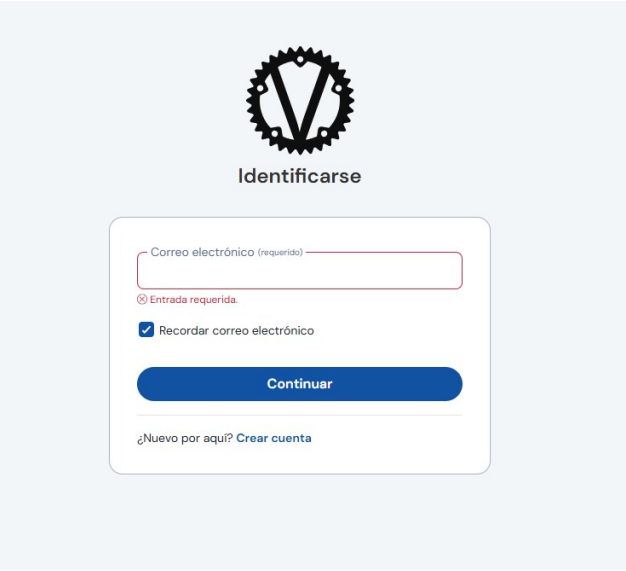
Ventaja para empleados:

Más seguro que anotar contraseñas en post-its o documentos.
Fácil de usar: Acceso rápido sin recordar decenas de claves.

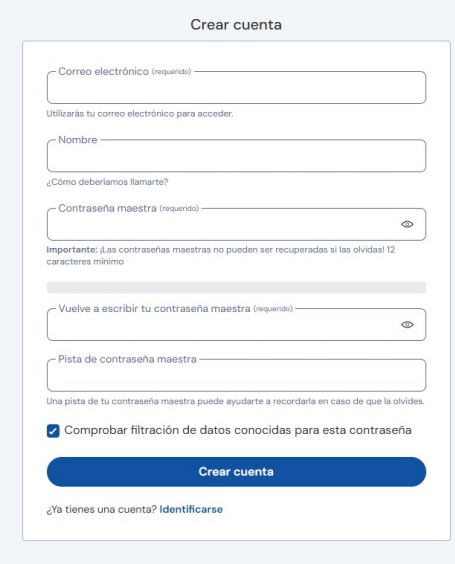
"Como una caja fuerte digital para tus contraseñas, pero más simple y controlada por la empresa."

Registro y acceso:

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



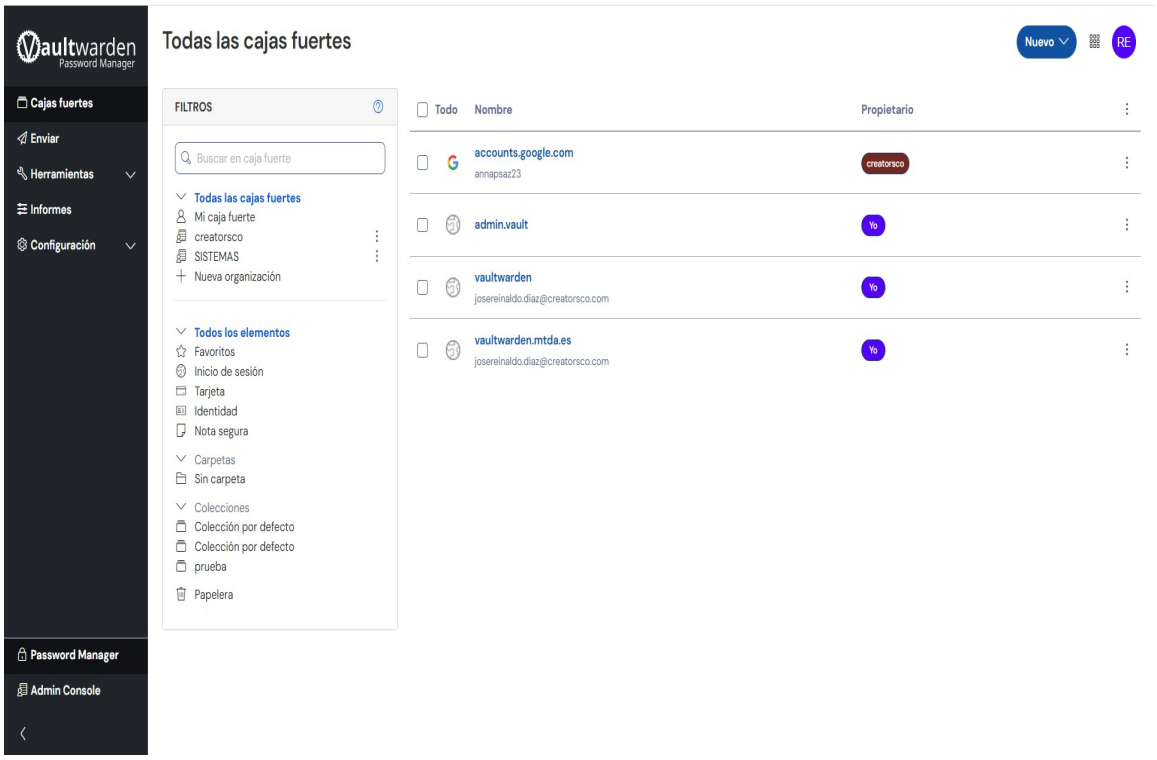
Aquí le daremos a crear una cuenta para registrarnos



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.

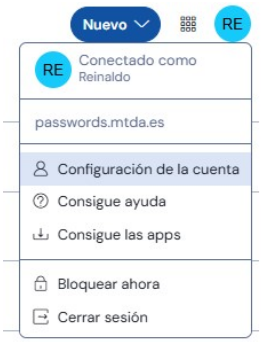
- **Iniciar sesión:** Después de crear tu cuenta, utiliza tus credenciales para acceder a la bóveda de contraseñas.

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.



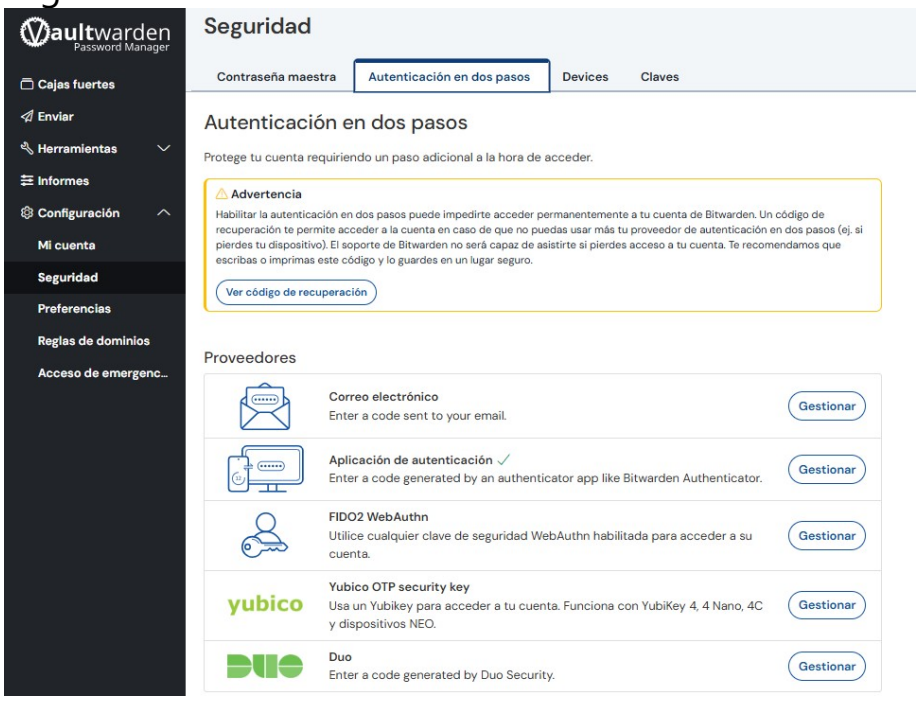
En el contenido para almacenar tenemos varias opciones: inicio de sesión, datos de tarjetas, identidad y notas seguras; la parte que más nos interesa es la de inicio de sesión

- 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



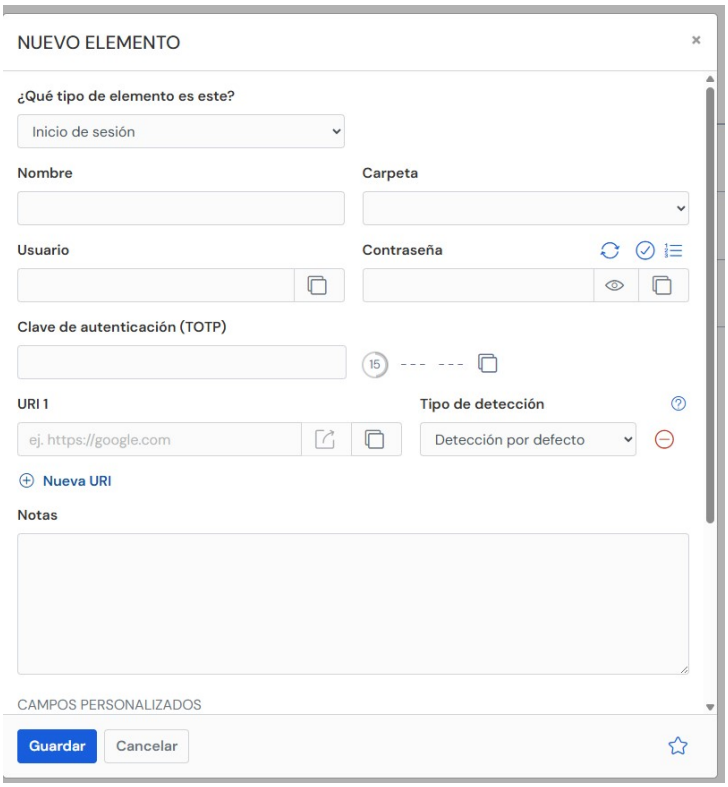
Una vez en el apartado **Autenticación en dos pasos**, se podrá elegir el método de verificación preferido:

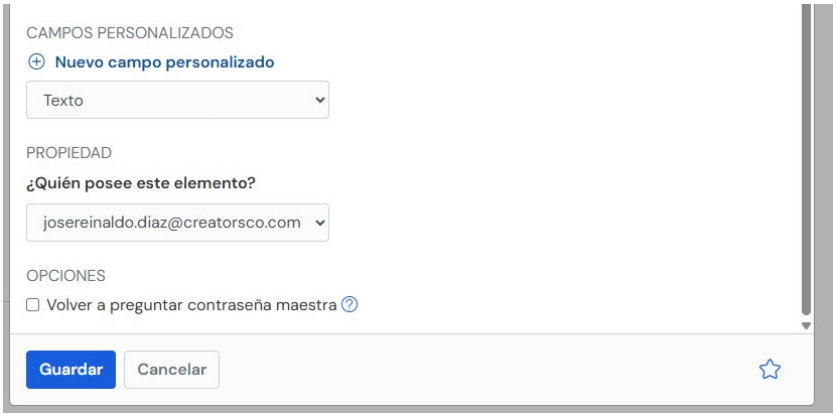
> **Correo electrónico**: el sistema enviará un código temporal al correo asociado a la cuenta. Dicho código deberá ser ingresado para completar el proceso de activación.
>
> **Aplicación de autenticación**: se mostrará un código QR que deberá ser escaneado con una aplicación compatible (como Google 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:

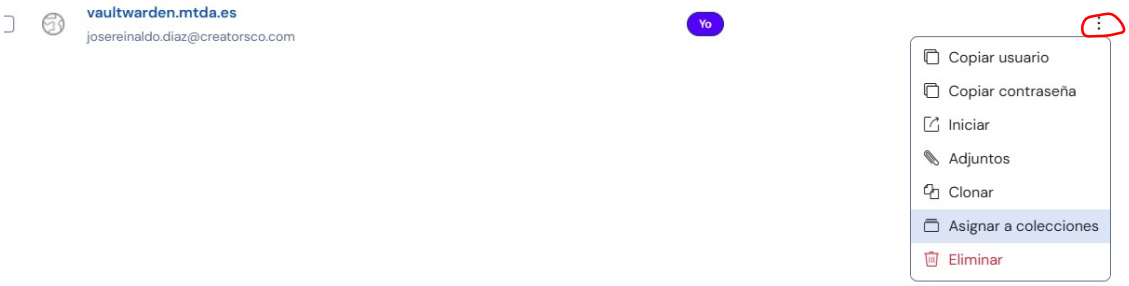
Para guardar contraseñas estas las podemos guardar en carpetas o en colecciones o directamente crearlas sin un directorio especifico, en vaultwarden las contraseñas son tratadas con el nombre de elementos, y para crear uno nuevo nos iremos a la esquina superior derecha y daremos a nuevo -> elemento

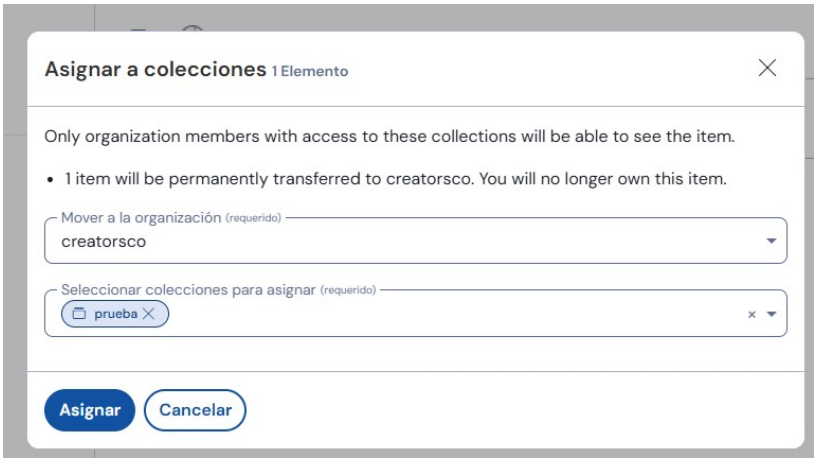




Una vez aquí ya nos sale para rellenar los datos de las credenciales y la configuración de auntenticación de la misma así como el dueño de la contraseña.

Una vez almacenada para compartirla lo que habría 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.

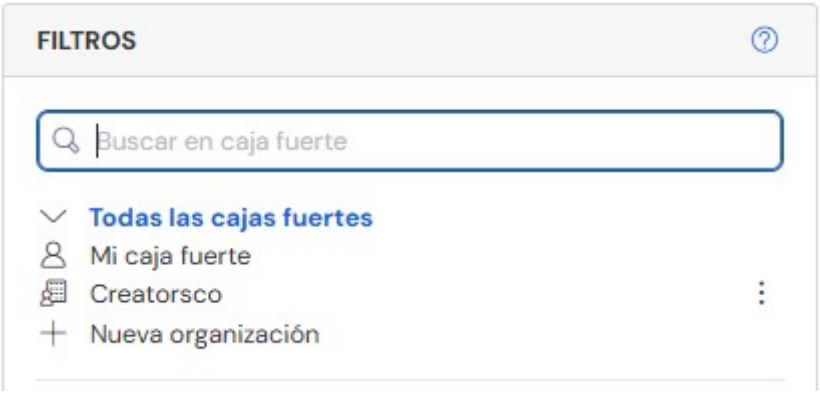




Y con esto ya estaría compartida la contraseña para todos los

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.



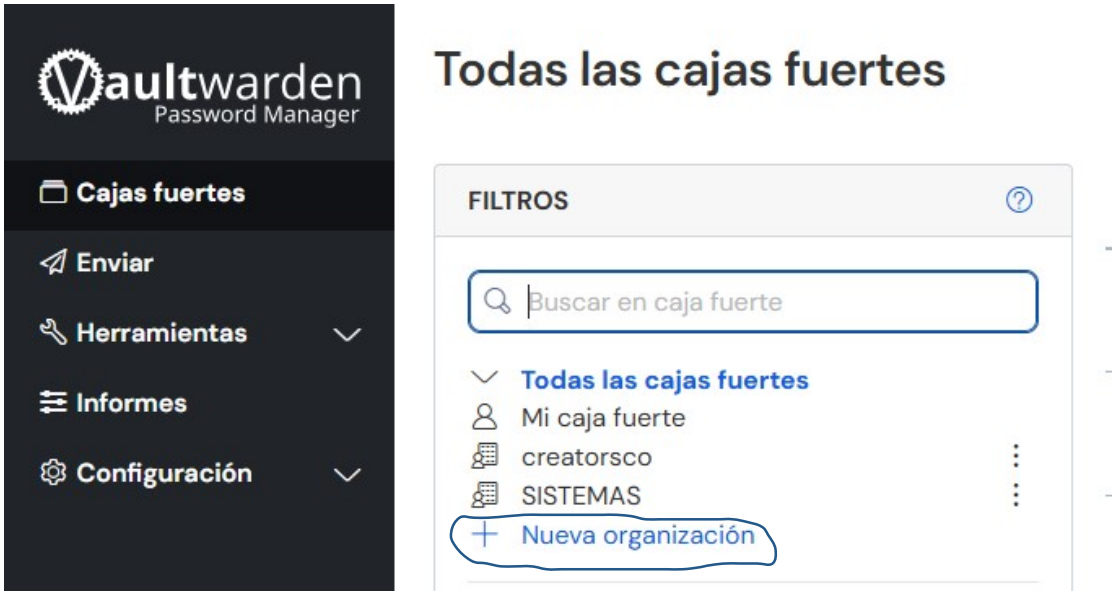
En el panel lateral, dentro del apartado "Filtros", se presentan las siguientes opciones de visualización:

- **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.

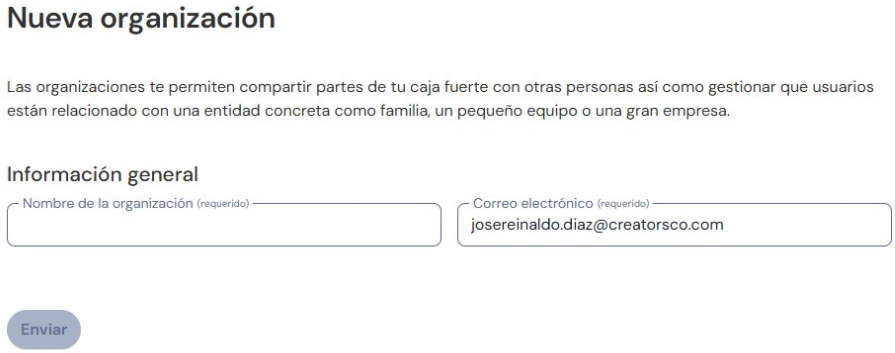
Organizaciones:

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:

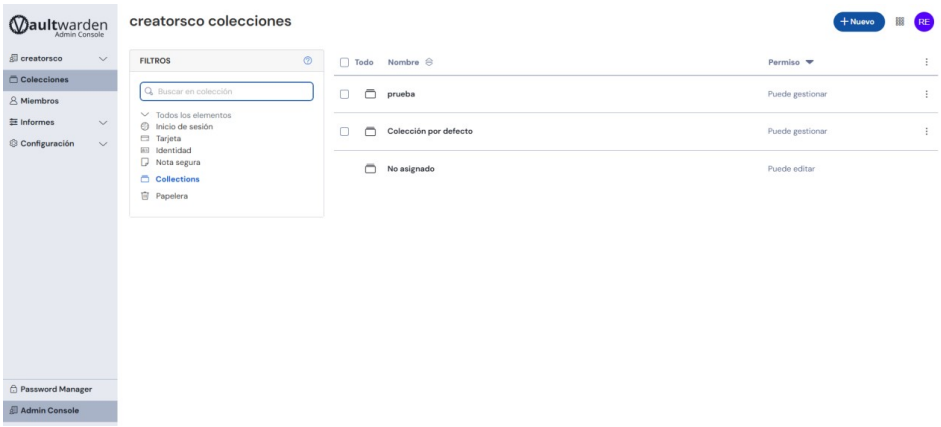
Primero que nada esto lo haremos con el usuario que sera admin de la administración; luego vamos a todas las cajas fuertes, y damos a “nueva organización”



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



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:

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, recupere 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.

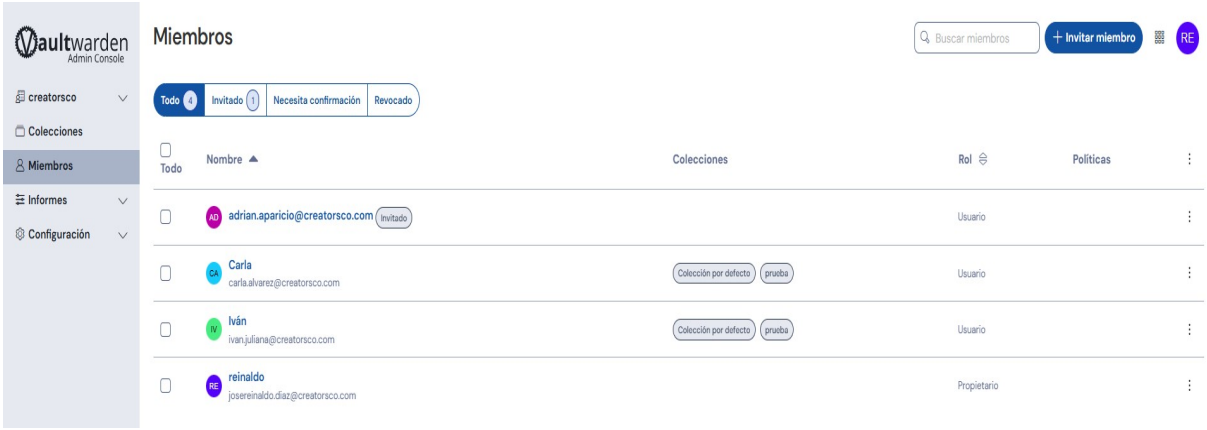
Exportar desde (requerido)
creatorsco

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



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.

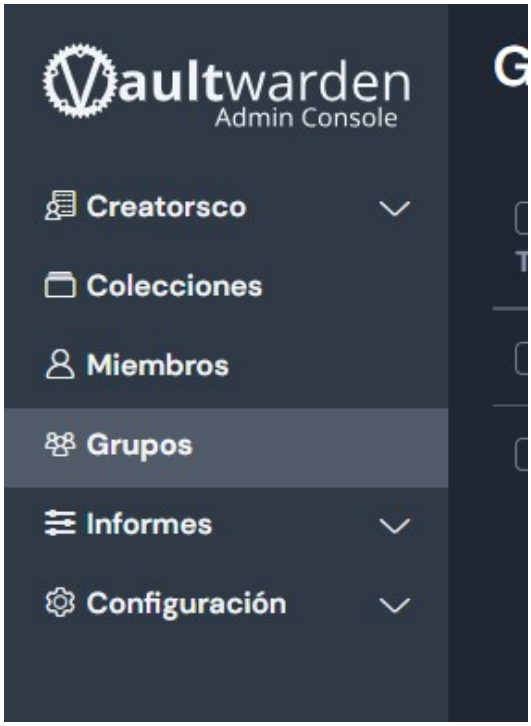
En la pestaña de **Colecciones**, podemos definir los permisos de cada usuario sobre las colecciones específicas a las que tendrá acceso. Los permisos disponibles son:

- **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.

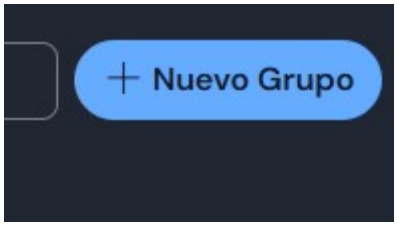
Una vez establecidos los permisos, simplemente se aplican a cada colección a la que el usuario tenga acceso el permiso especifico, garantizando que cada miembro tenga el nivel de acceso adecuado.

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.

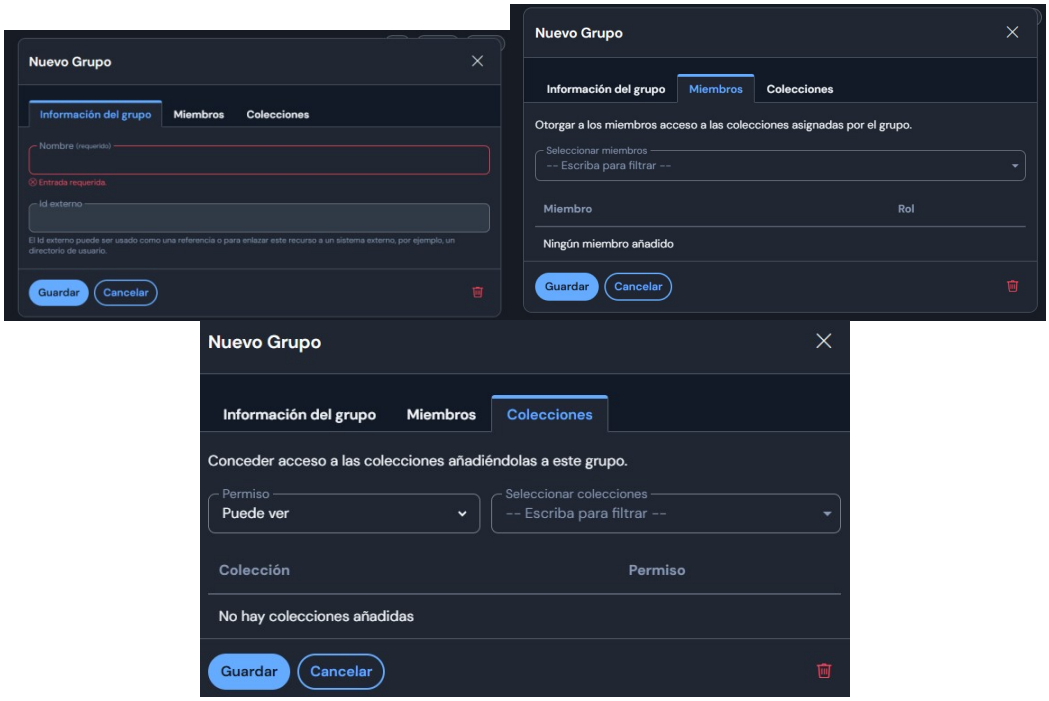
Para crear un nuevo grupo, el proceso es similar al de añadir una colección. Lo primero que debemos hacer es hacer clic en el botón que dice **"Nuevo grupo".**



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 configuramos los permisos correspondientes.

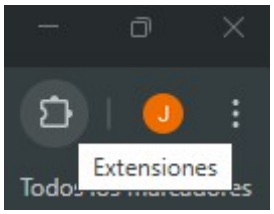
Una vez completados estos datos, el grupo quedará configurado y listo para usarse.

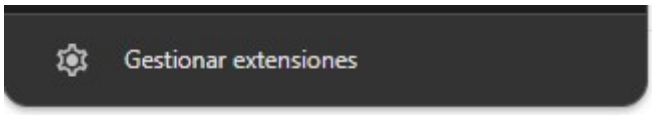


Configuración de navegador

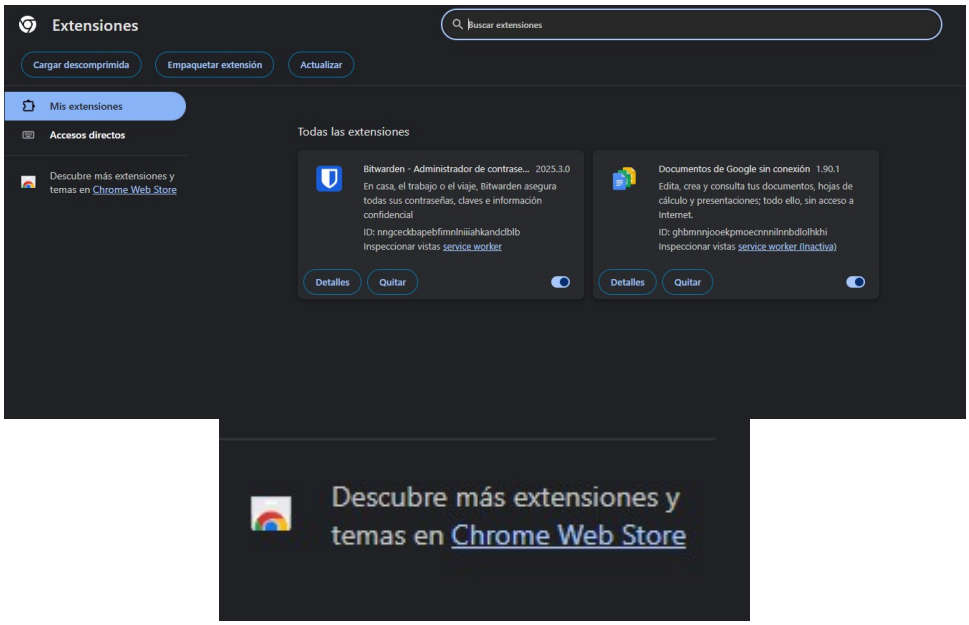
A continuación, debemos proceder con la configuración de la extensión de Bitwarden en el navegador. Esto nos permitirá utilizar nuestro gestor de contraseñas y que este se encargue de completar automáticamente las credenciales en los distintos sitios web.

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



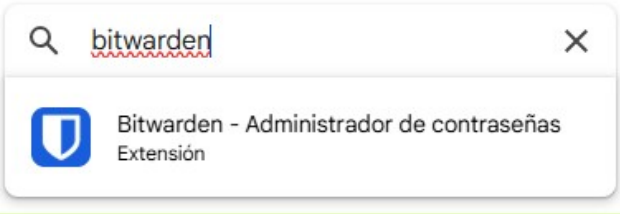


Al hacer clic en el icono de extensiones, se abrirá una ventana en la que podremos ver las extensiones instaladas en nuestro navegador. En mi caso, la extensión de Bitwarden ya aparece porque la he configurado previamente; sin embargo, es probable que no aparezca en el suyo. Para instalarla, deben hacer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



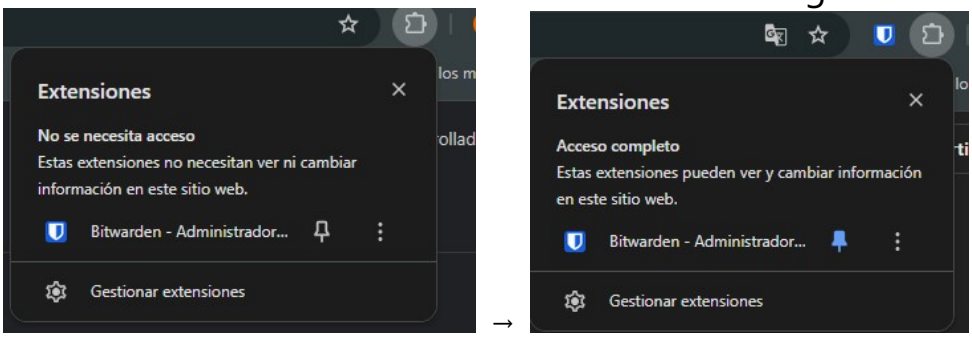
https://chromewebstore.google.com/category/extensions?utm_source=ext_sidebar&hl=es

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

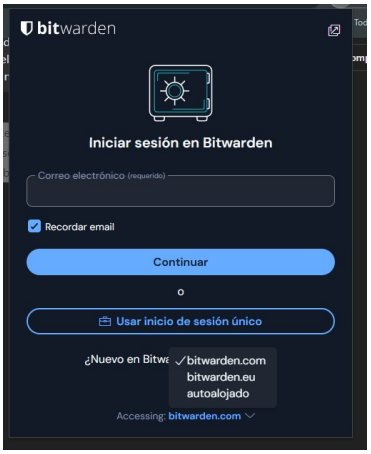


A continuación, seleccionamos la extensión de Bitwarden y hacemos clic en el botón de "Instalar" para añadirla a nuestro navegador.

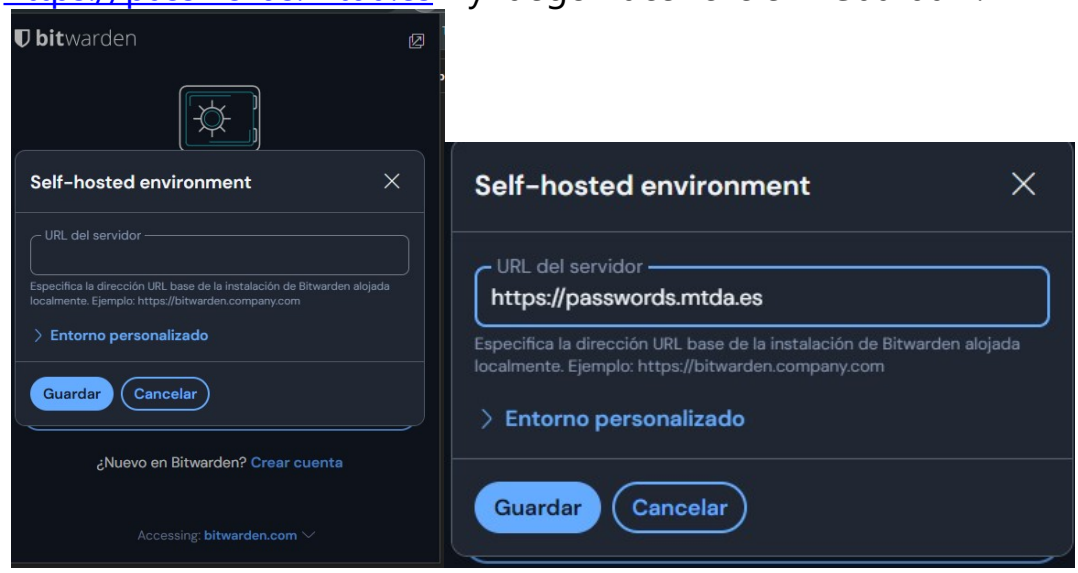
Una vez que la extensión esté instalada, volvemos a hacer clic en el icono de las extensiones en el navegador. Ahora debería aparecer la extensión de Bitwarden. Para facilitar su acceso, hacemos clic en el icono del alfiler para que la extensión se muestre de manera predeterminada en la barra de herramientas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



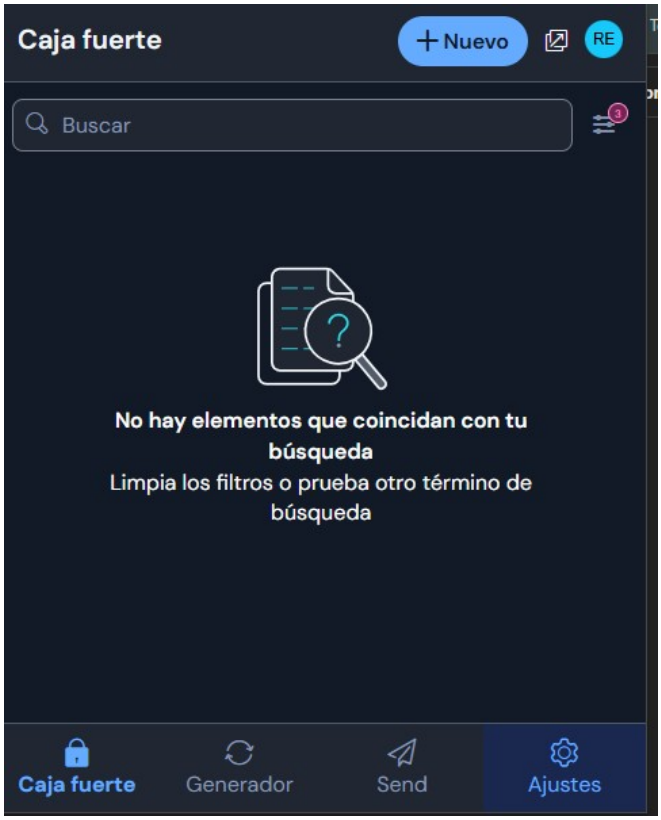
Con esto completado, abrimos la extensión y lo primero que debemos hacer es dirigirnos a la parte inferior, donde aparece la opción "Accessing". Allí, cambiamos la configuración de "Bitwarden" a "Autoalojado".



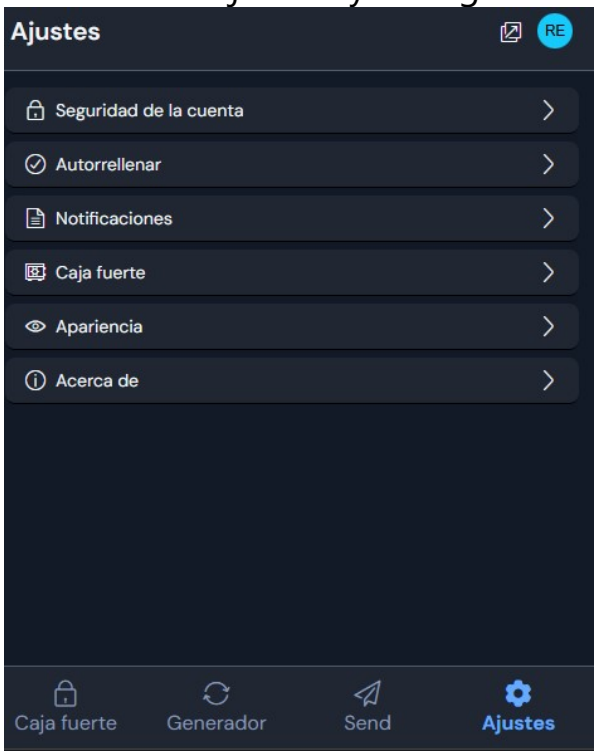
Al seleccionar la opción "Autoalojado", se nos pedirá la URL del servidor. Debemos copiar y pegar la siguiente dirección: "https://passwords.mtda.es" y luego hacer clic en "Guardar".



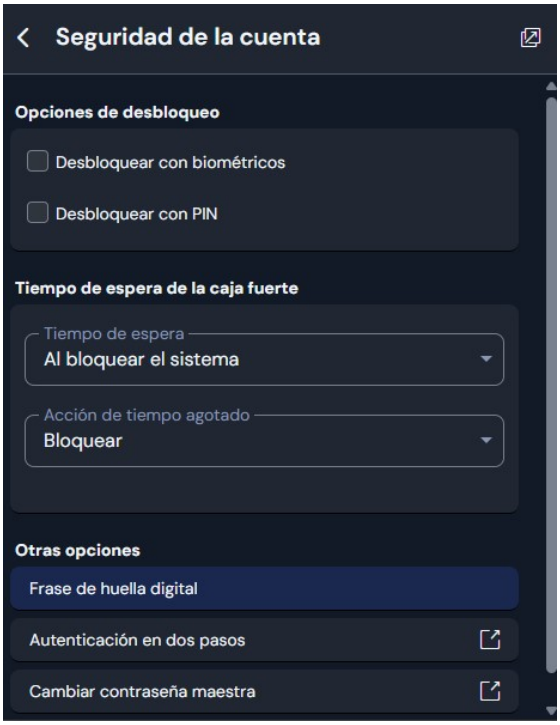
De esta manera, el diseño de la interfaz cambiará ligeramente. Lo único que nos quedará por hacer es acceder a nuestra cuenta utilizando nuestro correo electrónico y contraseña. Una vez hecho esto, nuestras credenciales deberían aparecer automáticamente en la extensión.



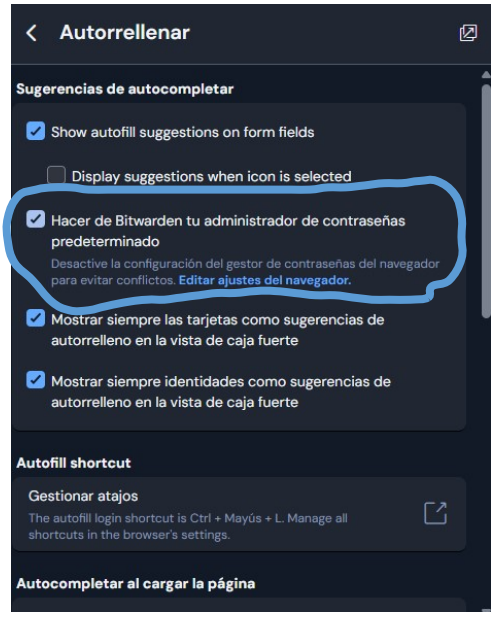
Una vez que hemos accedido, lo único que nos queda es realizar una pequeña configuración dentro de la extensión. Para ello, debemos ir a la sección de "Ajustes" y configurar lo siguiente:

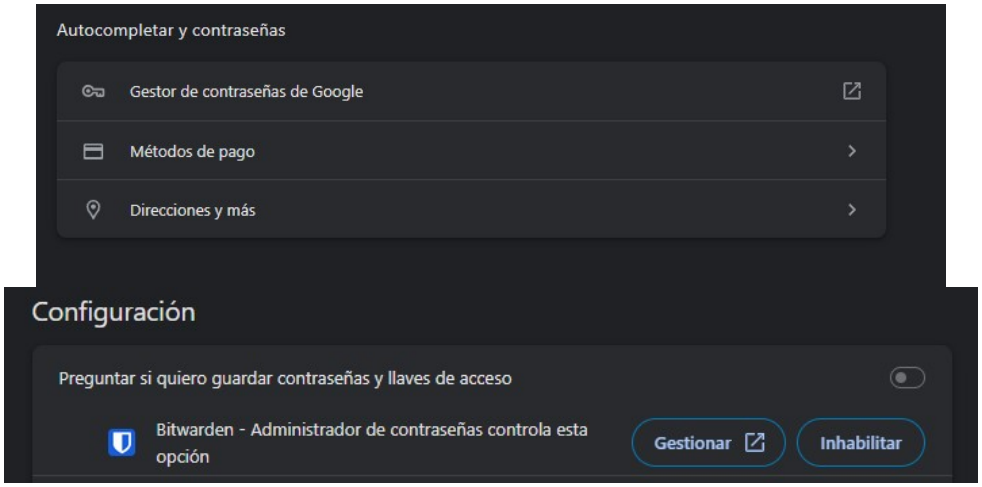


1. **Seguridad de la cuenta**: En esta sección, estableceremos el tiempo de espera de la aplicación. Configuramos este valor de la siguiente manera:



2. **Autorrellenar**: 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 icono 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.