

Gestores de contraseñas

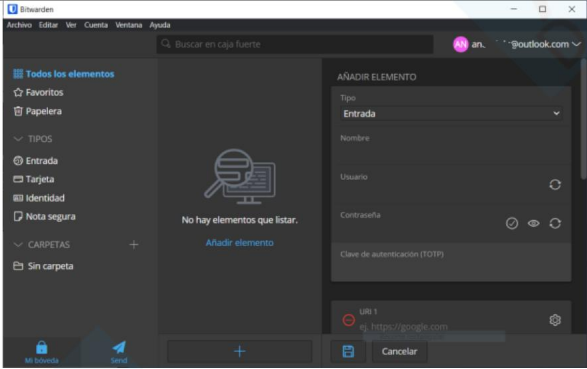
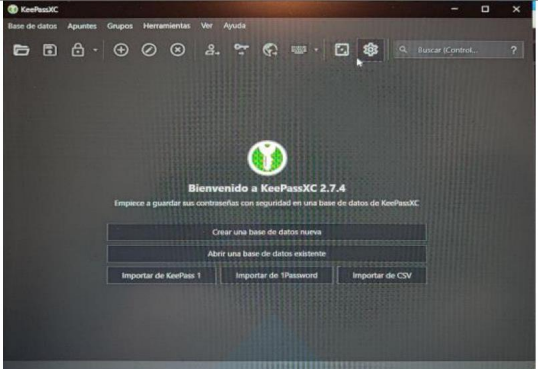

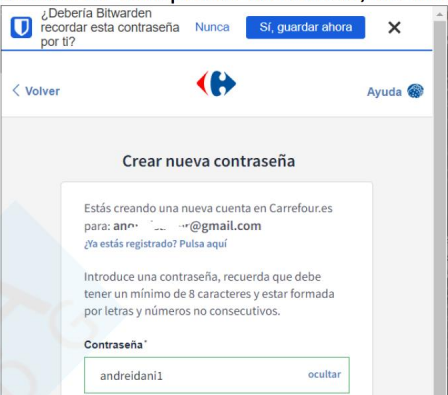

A.D.G.

Usa bitwarden y keepassXC

Explica las diferencias, posibilidades, centrate en:

- facilidad de uso, clientes posibles, extensiones en navegador, aplicacion de móvil

1) Accesos/Base de datos/Introducción de datos

BitWarden	KeePass
 <p>Pide un registro, no deja otra opción, por tanto tiene alojamiento en el que guarda la base de datos de la información de todas nuestras credenciales para acceder, desde la clave maestra hasta las claves de los sitios donde vayamos accediendo.</p>	 <p>A simple vista no veo ningún registro y eso da a entender que es un programa que actúa con archivos que tengamos en nuestro ordenador, nada de en otros alojamientos. Ahí ya depende de nosotros la seguridad que le pongamos al archivo de la base de datos, dónde lo guardamos si en el ordena, en un pendrive...</p>
 <p>También tiene una opción de inicio de sesión empresarial en el que supongo que la empresa otorgará esos datos a introducir y con ello les dará acceso a lo que quieran y necesiten ellos dependiendo de sus departamentos.</p> <p>Tiene distintos tipos de datos a guardar dependiendo de qué trate nuestra información: de completar identidad, de inicios de sesión...</p> 	 <p>Se puede elegir un cifrado más complejo y por tanto más difícil de descifrar, pero nos avisa de que también con ello tardará más. También puede elegirse el cifrado:</p>

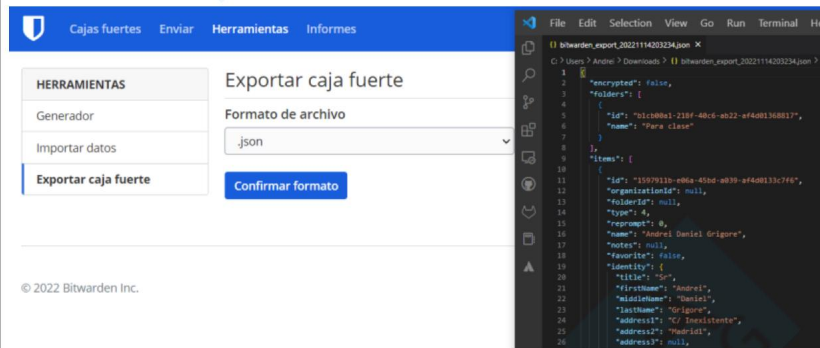
Es mejor la detección que hace automática de los sitios a los que accedemos y por tanto las urls en el caso de usar su Extensión por ejemplo en Chrome, ingresos automáticos de la información como en este caso la clave, en vez de tener que ingresar e indagar para saber qué url poner, volverla a escribir, etc. Esto mejora la rapidez, es más intuitivo y sencillo.

En el caso de usar la aplicación de Windows es menos sencillo que estar en una misma página y hacer un click como es en la extensión, hay que añadir más datos pero podemos usar una detección por defecto que es útil si no sabemos dónde se encuentra el lugar donde tenemos que iniciar sesión.

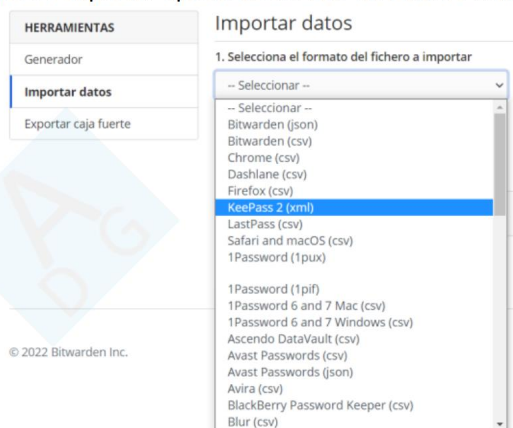
Tiene posibilidades de personalizar una contraseña generada automáticamente por longitudes y tipos de caracteres. También por frase de distintas palabras. Mi inicio de sesión tiene también una frase de huella digital generada.

También da la opción de añadir un fichero extra de clave con unos bytes aleatorios dentro para más seguridad en el inicio de sesión.

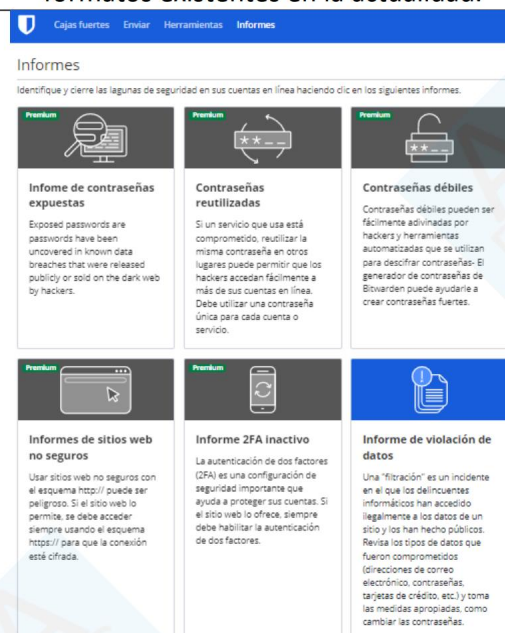
Se puede crear grupos para diferenciar las claves o información que vamos guardando para nuestros inicios de sesión, ajustando su nombre, iconos, luego al introducir la clave se añaden título, etiquetas...



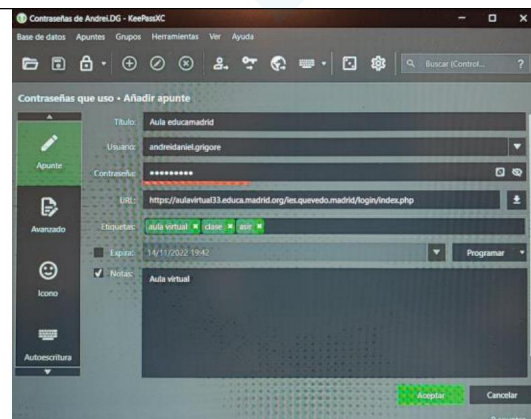
La exportación es muy sencilla para exportar los datos que tengamos y queramos hacer por ejemplo una copia de la base de datos en nuestro ordenador, pendrive, etc... pero claro depende de la forma del guardado del mismo (sin clave, sin cifrado, si se usará más o se guardará en un cajón...) dependerá nuestra seguridad de los datos. Tenemos distintos tipos de formato de exportación en json, json encriptado, o csv, en KeePassXC se podrá exportar aparte de en CSV en HTML o XML.



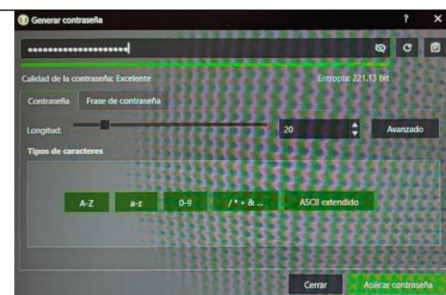
Para la importación podremos usar los de muchísimos tipos de formatos existentes en la actualidad.



Tenemos muchos informes que podemos generar de distintas necesidades, a comparación de KeePassXC que sólo Contraseñas débiles tenía. Sin embargo, estas funciones son Premium.



Es una forma un tanto difícil de estar ingresando los datos cada vez en vez de tener una detección automática del sitio en el que nos encontramos iniciando sesión o registrándonos, o simplemente que queremos tenerlo añadido a nuestra base de datos para un futuro uso. Por ello más adelante instalaré la extensión y mostraré un poco el hacerlo automático.



Tiene un sistema de generar contraseñas personalizables dependiendo de qué caracteres queremos que tenga, longitud... también podemos hacer que sea una contraseña en tipo de frase donde se nos expande las posibilidades de personalización.

Informe de violación de datos

Una "filtración" es un incidente en el que los delincuentes informáticos han accedido ilegalmente a los datos de un sitio y los han hecho públicos. Revisa los tipos de datos que fueron comprometidos (direcciones de correo electrónico, contraseñas, tarjetas de crédito, etc.) y toma las medidas apropiadas, como cambiar las contraseñas.

Usuario




and-...@gmail.com

Verifica cualquier nombre de usuario o dirección de correo electrónico que utilices.

Comprobar filtraciones

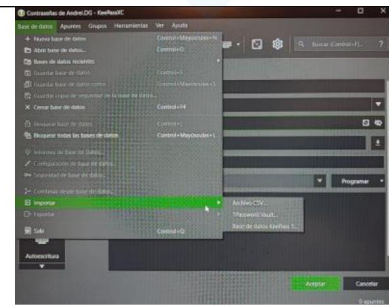
CUENTAS COMPROMETIDAS ENCONTRADAS

and-...@gmail.com fue encontrado en 3 filtración/es de datos en línea.

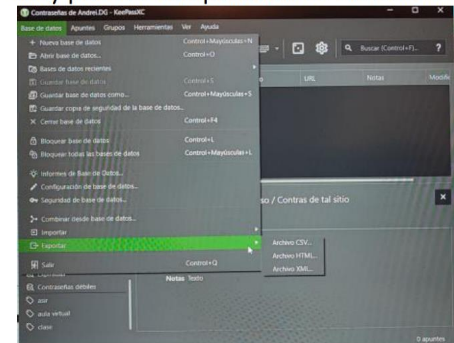
 <p>Daily Quiz In January 2021, the quiz website Daily Quiz suffered a data breach that exposed over 8 million unique email addresses. The data also included usernames, IP addresses and passwords stored in plain text.</p> <p>Datos comprometidos:</p> <ul style="list-style-type: none"> Email addresses IP addresses Passwords Usernames 	<p>Página web dailyquiz.me</p> <p>Usuarios afectados 8.032.404</p> <p>Se ha producido una filtración 13 ene 2021</p> <p>Filtración reportada 21 may 2021</p>
 <p>Jobandtalent In approximately February 2018, the employment website Jobandtalent suffered a data breach which then appeared for sale alongside other breaches a year later. The incident impacted 11 million subscribers and exposed their names, email and IP addresses and passwords stored as salted SHA-1 hashes.</p> <p>Datos comprometidos:</p> <ul style="list-style-type: none"> Email addresses IP addresses Names Passwords 	<p>Página web jobandtalent.com</p> <p>Usuarios afectados 10.981.207</p> <p>Se ha producido una filtración 1 feb 2018</p> <p>Filtración reportada 17 ene 2021</p>
 <p>Nitro In September 2020, the Nitro PDF service suffered a massive data breach which exposed over 70 million unique email addresses. The breach also exposed names, bryopt password hashes and the titles of converted documents. The data was provided to HIBP by dehashed.com.</p> <p>Datos comprometidos:</p> <ul style="list-style-type: none"> Email addresses Names Passwords 	<p>Página web gonitro.com</p> <p>Usuarios afectados 77.159.696</p> <p>Se ha producido una filtración 28 sept 2020</p> <p>Filtración reportada 19 ene 2021</p>

Volver a los informes

Dispone de un apartado integrado para saber si has sido pwneado directamente desde su extensión.



Tiene unos pocos formatos de importado de archivos, muy pocos a comparación de BitWarden.



En la exportación comparte solamente 1 opción de las que ofrece BitWarden que es CSV. Luego está HTML y XML.

CREAR NUEVO SEND

Nombre

Para enviar

Un nombre amigable para describir este Envío.

¿Qué tipo de Send es este?

☒ Archivo

☐ Texto

Archivo

Seleccionar archivo Ninguno archivo selec.

El archivo que desea enviar. El tamaño máximo de archivo es de 500MB.

COMPARTIR

☒ Copia el enlace para compartir este envío a mi portapapeles al guardar.

OPCIONES

Fecha de eliminación

7 días

Fecha de Expiración

Nunca

El envío se eliminará permanentemente en la fecha y hora especificadas.

Número máximo de accesos

Si se establece, los usuarios ya no podrán acceder a este envío una vez que se alcance el número máximo de accesos.

Contraseña

Opcionalmente se requiere una contraseña para que los usuarios accedan a este Envío.

Notas

Notas privadas sobre este Envío.

☐ Ocultar mi dirección de correo electrónico a los destinatarios.

☐ Deshabilita este envío para que nadie pueda acceder a él.

Guardar Cancelar

También puede programar un envío de un archivo o texto y elegir la validez, cantidad de personas que podrán acceder o descargar, la contraseña para el mismo...

Bitwarden Send

Usuario andri...@outlook.com de Bitwarden compartió contigo

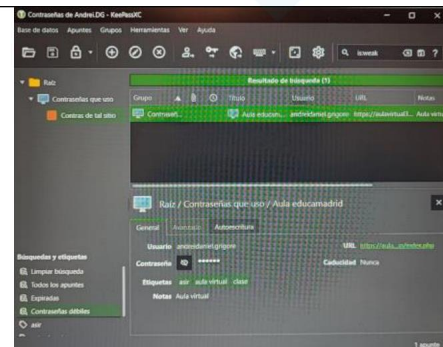
Para enviar

Hola

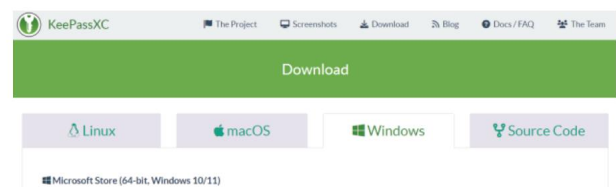
Copiar valor

Bitwarden Send transmite información sensible y temporal a otros de forma fácil y segura. Aprende más sobre Bitwarden Send o registrarse pruébalo hoy.

© 2022 Bitwarden Inc. Versión 2022.10.2

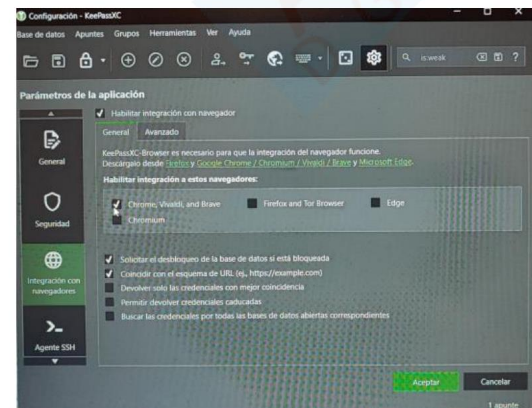


Podemos ver un apartado de Contraseñas débiles por ejemplo, que nos filtra las contraseñas guardadas por si hay alguna que no sea muy fuerte y queramos cambiarla.

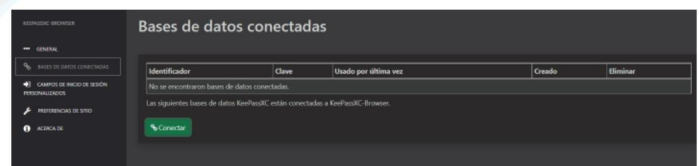


Tiene distintos dispositivos y softwares por consiguiente. También hay extensión para el navegador.

Para hacerlo funcionar en el navegador.



Luego conectar la base de datos en Chrome en mi caso:



La extensión es oficial de KeePassXC al menos en Chrome, pero habrán otros navegadores en los que no sea oficial sino de otras personas o comunidades. Igual pasa en la Play Store porque no encuentro ninguna con ese nombre, habrán de terceros y entonces ya ahí hay una seguridad que se va perdiendo y nunca se sabrá hasta qué nivel.

Desktop

Access Bitwarden on Windows, macOS, and Linux desktops with native applications.

Windows

Support for Windows 8, 10, and 11

macOS

Support for macOS 10.14+ and Safari 14+

Linux

Support for most distributions

more desktop installation options

Web Browser

Integrate Bitwarden directly into your favorite browser with browser extensions for a seamless browsing experience.

Google Chrome

Safari

Mozilla Firefox

Vivaldi

Opera

Brave

Microsoft Edge

Tor Browser

Mobile

Take your password manager on the go with mobile apps for your phone or tablet.

Tiene múltiples dispositivos y softwares compatibles. Son oficiales tanto las aplicaciones como las extensiones en los distintos sistemas base o navegadores.

Si nos olvidamos de la contraseña maestra, el archivo que hayamos usado adicionalmente para la clave, en KeePassXC es imposible de volver a recuperarla, y obviamente si perdemos la base de datos, también.

Si perdemos la contraseña maestra es posible recuperarla y acordarnos de algún modo, por ejemplo con las pistas. También podríamos compartir las contraseñas con otras personas, por tanto no seríamos los únicos los que las tendríamos así que sería posible recuperarlas, esto último sólo sería con Premium.

Ajustes

Tiempo de espera de la caja fuerte

Al reiniciar el navegador

Acción de tiempo de espera de la caja fuerte

Bloquear

Desbloquear con PIN

Desbloquear con biométricos

Bloquear

Autenticación en dos pasos

CUENTA

Membresía Premium

Cambiar contraseña maestra

Frase de huella digital

Cerrar sesión

HERRAMIENTAS

Pestaña

Caja fuerte

Send

Generador

Ajustes

Para ello podríamos ayudarnos de otros métodos de acceso, que sería como un método de recuperación también, ya sea por PIN, con huella, autenticación en dos pasos (que sólo permite BitWarden por ej)

Me gusta más la interfaz que tiene bitwarden, también la puedes personalizar los modos de vista claros oscuros...Es más intuitiva pero aparte tiene más organización en cuanto a los apartados, menús...

Se puede introducir distintos datos

KEEPASSXC - BROWSER

Configuración general

*** GENERAL

BASES DE DATOS CONECTADAS

CAMPOS DE INICIO DE SESIÓN PERSONALIZADOS

PREFERENCIAS DE SITIO

ACERCA DE

Interfaz de usuario

Color del tema

Sistema

✓ Activar iconos del campo nombre de usuario.

Añadir como icono a los campos de nombre de usuario para rel

Activar iconos generador de contraseñas.

Contraseñas nuevo - KeePassXC

Base de datos

Apuntes

Grupos

Herramientas

Ver

Ayuda

Tema

Modo compacto

Siempre encima

✓ Mostrar panel de previsualización

✓ Ocultar usuarios

✓ Ocultar contraseñas

Automático

Claro

Oscuro

Clásico (Plataforma-nativo)

Control+Mayúsculas+A

Control+Mayúsculas+B

Control+Mayúsculas+C

Autoescritura

Buscando...

Caducidad

Notas

Activado

Activado

Nunca

Búsquedas y etiquetas

Limpiar búsqueda

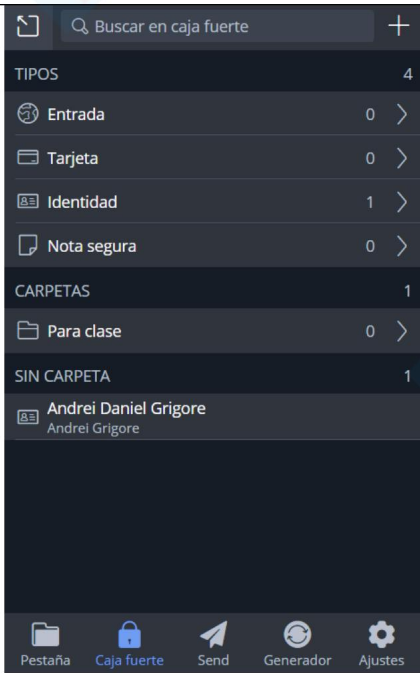
Todos los apuntes

Expiradas

Contraseñas débil

0 apuntes

Tiene alguna que otra configuración de personalizar por ejemplo en el programa de Windows, o en la extensión de Chrome de aparecer modo claro, oscuro..



En la aplicación de BitWarden oficial en la Play store de Android puedo también activar el acceso por la huella de mi dedo

