



BLOQUE 1
Qué es
FIELD 011 - KEEPASSXC
ITINERARY MY FAMILY



npub1u04jat9y9qshycawfxe93sz5p2j0d7upmmqg76wxvnqlp39ffqqss0jphc





Contenido

Bloque 1: Qué es

- 1.1 Gestor de Contraseñas.
- 1.2 Por qué los necesitamos.
- 1.3 Sincronización.
- 1.4 Dispositivos.



Descargo de responsabilidad: *Todo lo tratado en estas páginas no tiene estatus de consejo de inversión, seguridad ni asesoramiento financiero ni de recomendación. Los nombres de productos, empresas y otros entes citados en estas páginas son ajenos a los autores y no existe relación alguna de los autores con ellos. Es deber del lector/aprendiz verificar la idoneidad y conveniencia de interactuar con ellos en cualquiera de sus formas. En ningún momento los autores son responsables de las decisiones que el lector/aprendiz tome en relación con su patrimonio, su seguridad, su privacidad y su propia integridad y de las consecuencias que se deriven de ello. Te recomendamos que hagas tu propio análisis, te generes un criterio propio y tomes tus propias decisiones soberanas de modo que seas tú el único responsable de las mismas.*





Bloque 1: Qué es

Hoy en día cualquiera de nosotros debe recordar numerosas contraseñas. Desde websites, tu email, tu servidor, diferentes accesos en servicios, etc. La lista es inmensa. Y en cada uno de ellos deberías usar una única contraseña.

Si no llevas a cabo este hábito o rutina tendrías un verdadero problema si un tercero se hace con tu única contraseña. En ese caso, al no usar contraseñas independientes para cada servicio, este actor tendría acceso a todas tus cuentas gracias a tus malas prácticas.

Este es el principal problema que muchos todavía no quieren afrontar por diferentes razones. Sin embargo, hoy día, la tecnología nos ofrece soluciones de código abierto como KeePassXC en la que poder hacer una gestión óptima, segura y privada de nuestras contraseñas.

Es harto difícil sino imposible recordar todas las contraseñas de todos los servicios que contratamos en nuestra vida. Para eso existen los gestores de contraseñas.

La dinámica de los gestores de contraseñas es la siguiente: **debes recordar únicamente una contraseña maestra - master key -** de modo que sea lo suficientemente **compleja** y **aleatoria** para que un atacante se disuada de atacarla y que a su vez sea lo suficientemente **recordable** de modo que no te suponga un incordio tener que acudir a consultarla cada vez que quieras hacer uso de tu gestor de contraseñas. Esta contraseña maestra es la llave para acceder a todas tus contraseñas restantes - que pueden ser todo lo complejas y aleatorias que necesites - porque no necesitarás recordarlas.

Repetimos: sólo necesitas una contraseña maestra recordable que abra el cofre o caja fuerte en el que se encuentran el resto de contraseñas de todos tus servicios.





1.1 Gestor de contraseñas

Existen numerosas soluciones de gestores de contraseñas en el mercado. Aunque todavía su uso no es extensivo entre toda la población.

Sin embargo, tu perteneces a esa franja puesto que si estás aquí es porque ya sabes de la necesidad de implementar esta solución tecnológica en tu esquema de seguridad y privacidad digitales.

Hemos tratado anteriormente diferentes soluciones de gestores de contraseñas. En el FIELD 010 – EMAIL *Protegiendo al Rey* desarrollamos nuestro esquema utilizando a fondo el gestor de contraseñas **PROTON PASS**.

Pero no es el único, también comentamos en las líneas de desarrollo futuras de este curso la posibilidad de implementar **BITWARDEN**. Si tienes dudas, puedes acudir al FIELD 012 – BITWARDEN para aprender más sobre esta opción.

Aquí desarrollaremos la solución de **KEEPASSXC** que es gratuita y de código abierto. Puedes consultar su código en su repositorio Github. Desde KEEPASSXC son firmes convencidos en que la seguridad de lo abierto al público es mucho mayor que cualquier código propietario o cerrado.

1.2 Por qué los necesitamos.

1. Necesitamos gestores de contraseñas porque no podemos recordar todas las contraseñas que generamos en nuestra vida.
2. Los necesitamos porque ofrecen una solución cifrada con los algoritmos de encriptación de los más seguros que existen AES-256, ChaCha20 y TwoFish.
3. Los necesitamos porque requerimos disponer de nuestras llaves digitales cada vez que tengamos

