Uso de gestores de contraseñas

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

GENERALITAT VALENCIANA

Unión Europea
Fondo Europeo de Desarrollo Regional
Una manera de hacer Europa

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Sobre CSIRT-CV

CSIRT-CV es el Centro de Seguridad TIC de la Comunitat Valenciana. Nace en junio del año 2007, como una apuesta de la **Generalitat Valenciana** por la seguridad en la red. Fue una iniciativa pionera al ser el primer centro de estas características que se creó en España para un ámbito autonómico.

Está formado por un equipo multidisciplinar de personal técnico especializado en los distintos ámbitos de la seguridad y dedicado a desarrollar medidas preventivas y reactivas para mitigar los incidentes de seguridad en sistemas de información dentro del ámbito de la Comunidad Valenciana, que abarca tanto la Administración Pública, como PYMES y ciudadanos.

Datos de contacto

CSIRT-CV Centro de Seguridad TIC de la Comunitat Valenciana
http://www.csirtcv.gva.es/
Generalitat de la Comunitat Valenciana,

Teléfono: +34-96-398-5300
Email: csirtcv@gva.es
https://www.facebook.com/csirtcv
https://twitter.com/csirtcv

Licencia de uso

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Índice de contenido

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Introducción

Hoy en día son muchas las contraseñas que gestionamos para acceder a todas nuestras cuentas (correo personal y corporativo, aplicaciones, redes sociales, etc.). El hecho de que no debamos utilizar la misma contraseña para todo, de que debemos utilizar contraseñas largas y con caracteres especiales, y de que las podemos necesitar en cualquier momento estemos en casa o no, hace que memorizarlas sea una tarea prácticamente inabordable.

Utilizar la misma contraseña para todo es extremadamente peligroso ya que si la descubren, capturan o directamente la obtienen de una web poco segura, podrán acceder a todos nuestros servicios online.

Guardarlas en un archivo de texto en el ordenador o móvil tampoco es una buena solución ya que aplicaciones, otros usuarios del dispositivo, o incluso el fabricante/servicio técnico, pueden llegar a tener acceso a dicho fichero.

En un mundo online, puede parecer que la mejor solución sea **anotar las contraseñas en una libreta**, pero esto también implica que en caso de perderla todas nuestras contraseñas queden expuestas, que las encuentren amigos o familiares, o que por la pérdida de la libreta nos quedemos sin acceso a todos nuestros servicios online.

Por estos motivos es recomendable la utilización de gestores de contraseñas: un gestor de contraseñas es una aplicación que se utiliza para almacenar y administrar todas nuestras contraseñas. La principal característica de este tipo de aplicaciones es que el fichero donde se guarda la información está cifrado con una contraseña maestra de forma que el usuario solo tiene que recordar **una clave para acceder a todas sus contraseñas**. El uso de estas herramientas fomenta que el usuario escoja claves complejas sin miedo a no ser capaz de recordarlas posteriormente.

Tal como hemos indicado, un gestor de contraseñas genera un fichero cifrado donde se almacenan los usuarios y contraseñas el cual debemos guardar a buen recaudo y hacer copias de seguridad periódicas en un USB o disco externo por si el fichero se pierde, borra, o deja de funcionar.

Otra característica común a la mayor parte de los gestores de contraseñas es que permiten generarlas aleatoriamente según los parámetros que le especifique el usuario (número de caracteres, uso de mayúsculas y minúsculas, caracteres especiales,…).

Algo que parece evidente pero que cabe recordar es la obligación de que la contraseña maestra del gestor de claves sea confidencial y lo suficientemente compleja para que no pueda ser descifrada o adivinada.

Elegir un gestor de contraseñas

A la hora de elegir un gestor de contraseñas adecuado, son varios los factores que debemos tener en cuenta.

En primer lugar debemos asegurarnos de que se trata de un software seguro que no va a permitir que ningún atacante (incluso la propia empresa que ha desarrollado el software) pueda acceder a nuestros datos. Para ello elegiremos programas que gocen de buena reputación, de desarrolladores de confianza, preferiblemente que no almacenen nuestras contraseñas online, y a ser posible cuyo **código fuente sea público** ya que este tipo de software permite que cualquiera pueda comprobar que el programa hace sólo lo que realmente dice.

Si bien es cierto que el 99% de los usuarios no tiene conocimientos para hacer estas comprobaciones, en caso de existir algún comportamiento sospechoso los que sí tienen capacidad de analizarlo podrían dar la voz de alarma, por lo que podemos tener relativa tranquilidad al respecto. Las herramientas que no son de software libre también son auditables pero el hecho de no disponer del código de la aplicación hace que la revisión de ésta sea más compleja y menos precisa.

Por otro lado debemos elegir una herramienta compatible con nuestro sistema

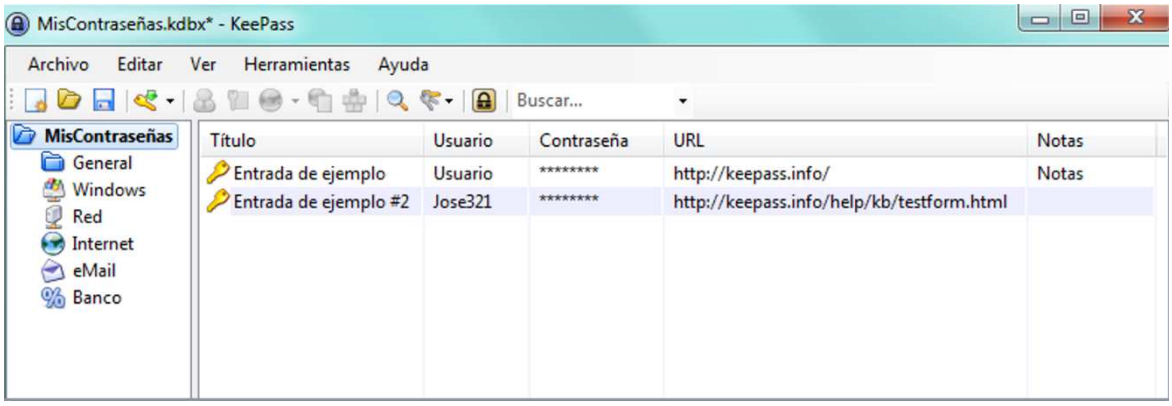
operativo y a ser posible en los dispositivos móviles que utilicemos, por lo que elegiremos software con versiones para Windows, Linux o Mac Os, según el caso, además de Android, iOS, etc…

Gestor de contraseñas recomendado

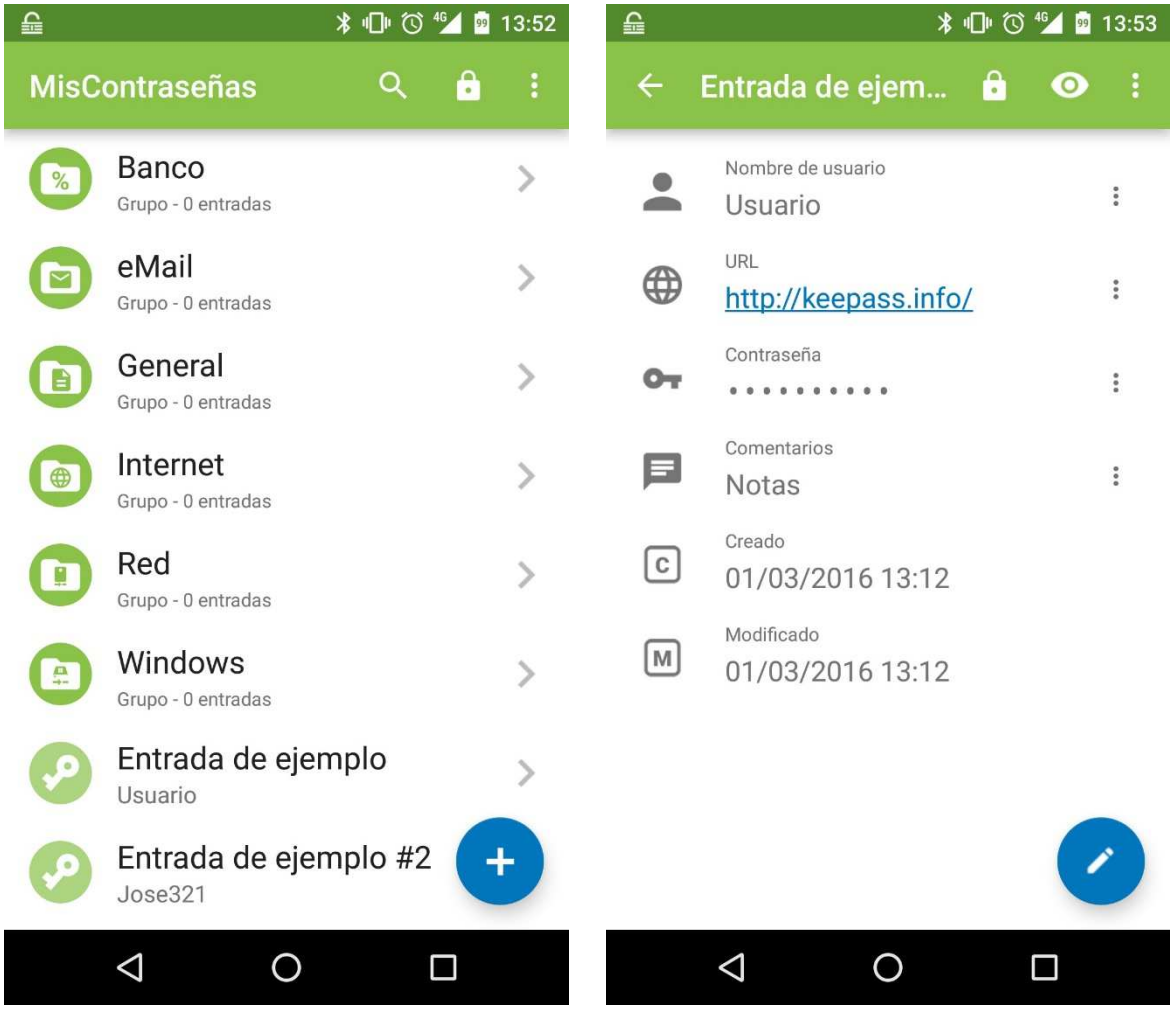
KeePass Password Safe http://keepass.info/

Probablemente se trata de la herramienta de software libre para gestión de contraseñas más utilizada, la cual almacena las contraseñas cifrándolas con los métodos de cifrado AES y Twofish.

KeePass nos permite organizar nuestras contraseñas en diferentes carpetas según el tipo de servicio al que den acceso. Permite también añadir direcciones web, notas, e incluso ficheros. Podemos adjuntar certificados digitales que queramos proteger, imágenes, o cualquier otro fichero que vayamos a necesitar para acceder a nuestros servicios.



Se encuenta disponible para Windows, Linux y Mac OS X. Al ser una herramienta de código abierto se han realizado versiones no oficiales pero estables y con ciertas garantías. Entre ellas cabe destacar KeePassX que fue un paso por delante en las versiones de Linux y Mac OS X, aunque también se encuentra disponible para Windows. Ambas aplicaciones son compatibles entre sí. También se han desarrollado versiones compatibles con KeePass para terminales móviles como Blackberry OS, Android o iOS y extensiones para navegadores como Keefox para Firefox.



Comentar por último que tanto KeePass como KeePassX están disponibles en español.

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

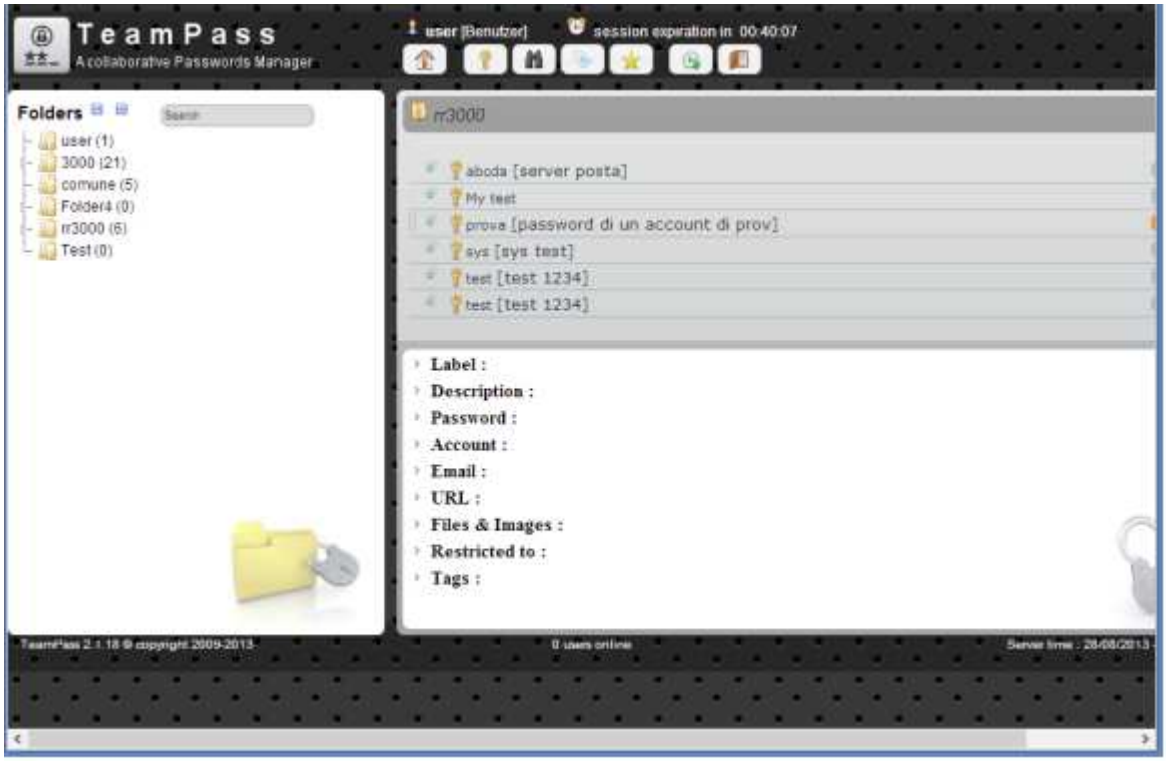
Gestores de contraseñas en la nube

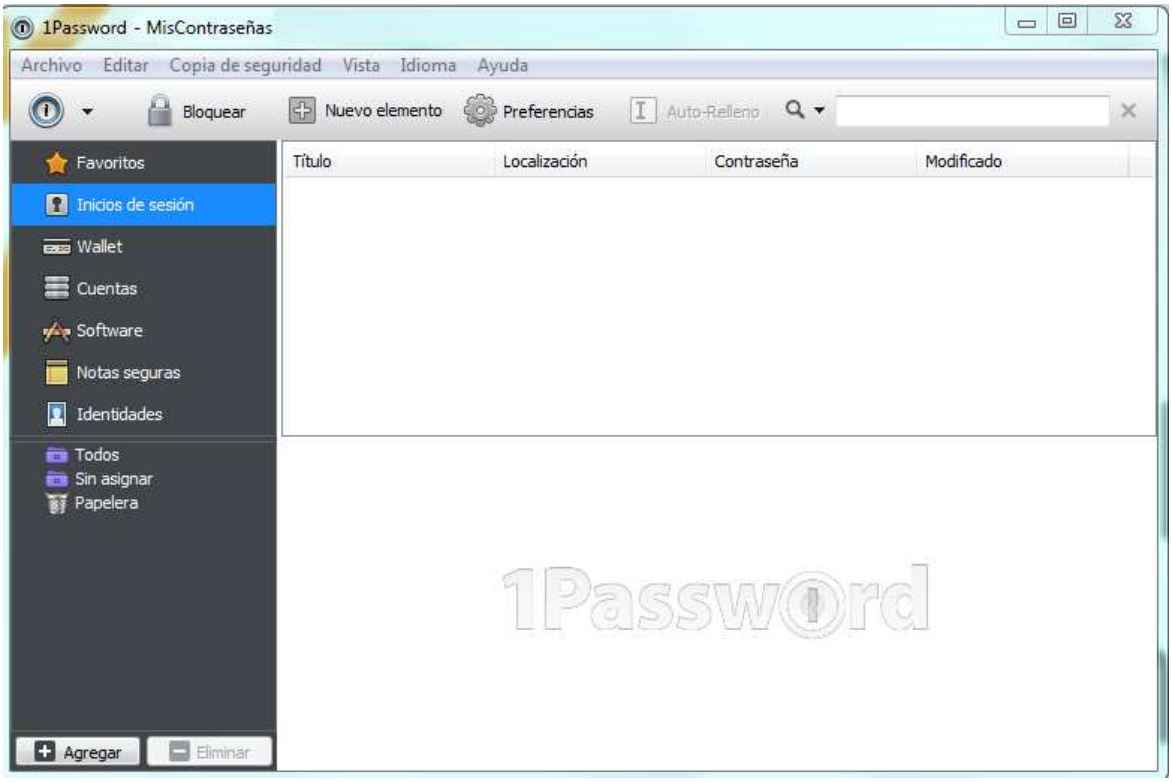
Cada vez están siendo más utilizados los gestores de contraseñas en un entorno *cloud*, lo que permite disponer en todo momento de las claves sea cual sea el lugar o el dispositivo desde el que se quiera acceder (aunque siempre será necesaria conexión a Internet).

Estos gestores tienen la principal ventaja de la disponibilidad, generalmente son multiusuario y la facilidad de acceso, pero también tienen sus desventajas. Una de ellas es respecto al control de las claves ya que al estar éstas en un servidor, una caída del servicio web podría provocar la imposibilidad de acceder a ellas.

Por otro lado, si bien pueden parecer soluciones más cómodas y versátiles que los gestores de contraseñas tradicionales, al utilizar este tipo de gestores existen importantes problemas de seguridad y confidencialidad a tener en cuenta. Estas empresas aseguran que no almacenan la clave maestra ni tienen acceso a los pares usuario-contraseña de manera clara, pero aunque esto sea así, estamos permitiendo que un tercero tenga almacenadas las contraseñas de las cuentas donde tenemos multitud de información personal (almacenamiento en la nube, correo, redes sociales,…) y que sea éste el responsable de la seguridad, la confidencialidad e integridad de los datos.

En cualquier caso, si fuera necesario utilizar algún gestor de este estilo cabe mencionar **TeamPass** (http://teampass.net) y **OnePassword** (https://agilebits.com/onepassword) las cuales cumplen con muchas medidas de seguridad como son el cifrado de datos y el protocolo seguro en las comunicaciones con el servidor.


TeamPass
A collaborative Passwords Manager
user [Benutzer]
session expiration in 00:40:07
Folders
user (1)
3000 (21)
comune (5)
Folder4 (0)
rr3000 (6)
Test (0)
rr3000
aboda [server posta]
My test
prova [password di un account di prov]
sys [sys test]
test [test 1234]
test [test 1234]
Label :
Description :
Password :
Account :
Email :
URL :
Files & Images :
Restricted to :
Tags :


1Password - MisContraseñas
Archivo Editar Copia de seguridad Vista Idioma Ayuda
Bloquear
Nuevo elemento
Preferencias
Auto-Relleno
Favoritos
Inicios de sesión
Wallet
Cuentas
Software
Notas seguras
Identidades
Todos
Sin asignar
Papelera
Título
Localización
Contraseña
Modificado
1Password
Agregar
Eliminar

CSIRT-CV
Centre Seguretat TIC
de la Comunitat Valenciana

Conclusiones

Este documento ha sido una breve guía para dar a conocer las herramientas de gestión de claves.

Se acostumbra a decir que las contraseñas son nuestras **llaves de acceso** a nuestras cuentas de Internet por lo que **deben ser lo más seguras posibles**: largas, complejas (preferiblemente con mayúsculas, minúsculas y caracteres especiales) y diferentes unas de otras con el fin de dificultar que la clave pueda ser descifrada o descubierta por terceras personas.

Resulta evidente que no se deben dejar anotadas en papel, ni almacenarlas en un fichero sin proteger del ordenador, ni mucho menos dárselas a nadie para que nos las recuerde en caso de olvido, por lo que para poder gestionar de forma segura nuestras contraseñas **desde CSIRT-CV aconsejamos la utilización de herramientas de gestión de claves y proteger el fichero con una única contraseña especialmente segura**.