Sociedad Andaluza para el Desarrollo de las Telecomunicaciones
CONSEJERÍA DE EMPLEO, EMPRESA Y COMERCIO

seguridad+ Y CONFIANZA DIGITAL | AndalucíaCERT CENTRO DE SEGURIDAD TIC

Informe de divulgación
Gestores de contraseñas

Tipo de documento:	*Informe*
Autor del documento:	*AndalucíaCERT*
Código del Documento:	*CERT-IF-10414–171124*
Edición:	*0*
Categoría	*Público*
Fecha de elaboración:	*24/11/2017*
N° de Páginas	*1 de 10*

1 TABLA DE CONTENIDOS

2 OBJETIVO

El objeto de este documento es proporcionar información a los usuarios acerca de los programas conocidos como Gestores de contraseñas, aplicaciones que se utilizan para almacenar parejas usuario/contraseña protegidas a través de una clave maestra.

3 ALCANCE

Este documento va dirigido tanto al personal de la Junta de Andalucía, como al público en general. Es de carácter divulgativo e informativo, en el cual se pretende dar a conocer los Gestores de contraseñas, de manera que el usuario sea consciente de cómo el uso de los mismos puede otorgarle mayor robustez a los distintos procesos de autenticación (login) en aquellas aplicaciones que utilice.

4 INTRODUCCIÓN.

El auge de Internet y la telefonía móvil han creado una nueva cultura digital en la que un usuario estándar maneja diariamente más de una decena de aplicaciones en las que se le requiere autenticación. Es habitual encontrar personas que disponen de cuentas registradas para:

- Cuentas de correo corporativo, cuentas de dominio Windows y otros sistemas Unix.

- Cuentas de servicios online (banca, redes sociales, ...).

Estos son solo algunos ejemplos de aplicaciones en las que el usuario habrá de iniciar sesión para poder acceder a su área personal. ¿Cómo manejar tantas cuentas y aún así recordar las credenciales de todas ellas? A menudo se opta por la alternativa más sencilla: usar para todo la misma pareja usuario/contraseña (o pequeñas variaciones de la misma que sean fáciles de recordar). Sin embargo, esta forma de proceder implica un grave problema de seguridad informática, ya que el compromiso de una cuenta en una aplicación concreta puede entonces hacerse extensible al resto, o al menos a buena parte de ellas. Una forma de solucionar este problema es a través de los **Gestores de contraseñas.**

5 GESTORES DE CONTRASEÑAS

Un gestor o administrador de contraseñas es un programa que se encarga de almacenar parejas usuario/contraseña. Para ello hace uso de una base de datos que se encuentra cifrada mediante una única clave conocida como *clave maestra*. De esta manera el usuario solo tiene que memorizar una clave para poder tener acceso a todas sus contraseñas almacenadas. Gracias a esto el usuario puede optar por tener distintas contraseñas para cada aplicación en la que se encuentre registrado y además haciendo uso de claves más complejas que sean más difíciles de romper.

Es común que sean los propios gestores de contraseñas los que ofrezcan la posibilidad de la generación de las mismas de manera automática, lo que favorece lo comentado anteriormente: el usuario puede crear contraseñas aleatorias robustas y a las que tener acceso de manera sencilla.

5.1 Seguridad en las contraseñas

Se ha comentado anteriormente que los gestores de contraseñas permiten la generación de contraseñas más robustas y seguras, evitando así posibles compromisos de cuenta, pero ¿qué hace que una contraseña sea segura? A continuación se dejan algunas pautas importantes en las que se basan los gestores de contraseñas a la hora de generar aleatoriamente las mismas, las cuales son configurables, por ejemplo:

- Longitud igual o superior a los 10 caracteres.
- Contener letras mayúsculas y minúsculas.
- Contener números y símbolos.
- Evitar caracteres repetidos y números consecutivos.

Si bien se ha mostrado la posibilidad que ofrecen los administradores de contraseñas para crear las mismas de manera aleatoria, también es habitual que sea el propio usuario el que cree sus contraseñas de manera manual para las aplicaciones de las que vaya a hacer uso y posteriormente las almacene en el gestor de contraseñas. En casos como este se recomienda, además de seguir las pautas de seguridad expuestas antes, lo siguiente:

- No usar información personal como nombres o fechas de nacimiento.
- Utilizar palabras o información que solo tengan sentido para el usuario, evitando combinaciones que puedan guardar relación entre sí.
- En caso de teclados españoles, aprovechar la letra ñ puede ser una buena opción para aumentar la complejidad.

5.2 Tipos de gestores de contraseñas

En función de dónde se encuentre instalado el Gestor de Contraseñas se pueden distinguir tres tipos de gestores:

- Software instalado localmente en el dispositivo.
- Gestores de contraseñas online.

- Dispositivos hardware basados en tokens.

5.2.1 Software instalado localmente en el dispositivo

Son aquellos gestores de contraseñas que residen instalados en el dispositivo del usuario como aplicaciones software, siendo estos dispositivos generalmente un ordenador o un móvil inteligente (smartphone). Estos gestores pueden funcionar sin estar conectados a la red, ya que la base de datos con las contraseñas es almacenada de manera independiente y localmente en el mismo dispositivo donde se encuentra instalado el gestor.

Existe también otra aproximación en la que el gestor de contraseñas se encuentra instalado en el dispositivo del usuario, pero requiere de conexión a Internet ya que la base de datos se encuentra almacenada remotamente en algún servicio de hosting.

5.2.2 Gestores de contraseñas online

Son servicios web que almacenan de manera segura las distintas credenciales del usuario. Su principal ventaja es que son accesibles sin necesidad de instalar ningún software, basta con que el usuario disponga de conexión a Internet y un navegador web. También juega a su favor el hecho de que se elimina el riesgo de robo de contraseñas por pérdida o sustracción del dispositivo (algo que sí puede ocurrir en los gestores instalados localmente o en los basados en tokens), aunque dada su ubicación remota el usuario debe confiar en el servidor de hosting. El hecho de que la base de datos se almacene en la nube puede implicar el riesgo de que la plataforma utilizada para guardar la información sea víctima de ciberataques dirigidos. Este fue el caso de la famosa LastPass en junio 2015, cuando la compañía admitió haber sido hackeada y recomendó a todos sus usuarios el cambio de su clave maestra.

5.2.3 Dispositivos hardware basados en tokens

Algo menos común que los dos anteriores, pero también utilizado. Se denominan tokens de seguridad o gestores de contraseñas basados en tokens, y se fundamentan en la idea de tener un dispositivo hardware al que se pueda acceder de manera local, como sería el caso de dispositivos USB o tarjetas inteligentes.

La base de datos de contraseñas se almacena en el token (se puede, por tanto, acceder a ella sin necesidad de conexión a Internet) de manera encriptada, evitando así el acceso y lectura no autorizados de la información. Es posible que los tokens requieran tener instalado en el terminal software específico con el que interactuar y los drivers adecuados para poder leer y decodificar los datos.

5.3 Sincronización

Dado que es común que el usuario utilice de manera simultánea distintos dispositivos (ordenador, móvil, tablet, etc), uno de los requisitos principales que se le exige a un buen gestor de contraseñas es que sea fácilmente accesible y utilizable desde distintos terminales. En función del tipo de gestor existen distintas formas de sincronizar la base de datos:

- En los gestores offline o totalmente locales (software y base de datos en el dispositivo) habrá de tener instalada la aplicación en todos los terminales de los que el usuario vaya a a hacer uso e importar/exportar la base de datos de contraseñas en los mismos. De esta manera se dispondrá de la información en los terminales de uso habituales.

- En los administradores locales pero con base de datos en la nube (software en el dispositivo, base de datos en servidor externo) la forma de proceder es tener instalada la aplicación en el dispositivo en uso y descargar la base de datos del servidor en que se encuentre alojada.

- En los gestores online (tanto el servicio como la base de datos son de acceso remoto) bastará con la autenticación en el servicio web que se use como gestor y se dispondrá de toda la información de credenciales. Para ello bastará con un navegador y conexión a Internet, independientemente del dispositivo que se esté utilizando.

- En los administradores basados en tokens las contraseñas viajan físicamente con el usuario que las transporta, por lo que siempre están a su disposición, aunque habrá de preocuparse de configurar correctamente todos los dispositivos en los que vaya a usar el token para que la lectura y decodificación se produzca correctamente.

5.4 Autologin

Una de las funcionalidades más interesantes de los gestores de contraseñas es la posibilidad de configurarlos para que hagan login de manera automática en los sitios webs que se especifiquen. Para ello bastará con descargar e instalar en el navegador el plugin del gestor que se esté utilizando y de manera sencilla se podrá iniciar sesión en los diferentes sitios web sin necesidad de introducir las credenciales cada vez.

6 GESTORES DE CONTRASEÑAS DE REFERENCIA

A lo largo de la sección anterior se ha explicado en qué consisten los administradores de contraseñas, los tipos que hay y cómo pueden utilizarse para que el aumento en seguridad no repercuta en un aumento de la complejidad con pérdida de comodidad para el usuario. Es el momento de mostrar de manera concreta algunos Gestores de contraseñas considerados de referencia por parte de los usuarios.

6.1 KeePass

KeePass es una utilidad de código abierto que mantiene las contraseñas cifradas en una base de datos local. Su punto fuerte es que todo se encuentra bajo control del usuario, ya que es un Gestor que se instala y actúa de manera local en el dispositivo. La desventaja es que obliga al usuario a que se preocupe de descargar manualmente los plugins para los navegadores y a encontrar una forma de sincronizar la base de datos de contraseñas entre distintos dispositivos.

Es un software preparado originalmente para sistemas Windows, aunque es multiplataforma y a día de hoy su instalación también es posible en Linux, MacOS, Android, IOs o Blackberry. Utiliza cifrado *AES 256* y *Twofish*. (aunque desde la versión 2.XX ya no está disponible). Es multilenguaje y permite almacenar y gestionar todas las contraseñas con una contraseña maestra como se ha explicado al principio. En últimas actualizaciones se ha añadido a sus funcionalidades el comparador de contraseñas (análisis de la calidad de las mismas), cuestión en la que flojeaba con respecto a otros gestores. Se pueden generar contraseñas aleatorias, añadir grupos de contraseñas, crear categorías, ver las últimas contraseñas modificadas, desactivar el autocompletado, etc.

6.2 LastPass

LastPass Password Manager nace en 2008 y posiblemente se ha convertido en el gestor de contraseñas más conocido del mundo en los últimos años. Es un gestor totalmente online, los datos se encuentran en la nube (la sincronización de la base de datos es sencilla, basta con contar con un navegador y conexión a Internet por lo que es completamente multiplataforma) y solo serán accesibles a través de la clave maestra. La seguridad de LastPass se basa en el cifrado con el algoritmo AES 256 bits localmente antes de ser enviado por *TLS* al servidor web. Con este encriptamiento local se logra que ni el propio gestor tenga constancia de cuales son las contraseñas del usuario. Adicionalmente a la clave maestra puede incluir *autentificación de dos factores*. También ofrece la posibilidad de usar *OTP (One Time Password)*. Cuenta con algunas opciones interesantes como su función de autocompletado en cualquier formulario o la prohibición del acceso desde la *red Tor.*

6.3 Dashlane

Dashlane surgió en 2011 y una de sus particularidades con respecto a otros gestores de contraseñas es que también puede actuar como monedero virtual, permitiendo los pagos en cualquier sitio web de manera segura. Es multiplataforma, aunque de manera limitada: hasta hace poco podía instalarse en Mac, Windows, Android e IOs, y recientemente ha incorporado Linux y Chromebook. A diferencia de LastPass es online, pero almacena los datos de manera local en el dispositivo. Desde el punto de vista de administrador de contraseñas funciona de manera análoga a los ya comentados, haciendo uso de una clave maestra para el descifrado de los datos. Adicionalmente puede incluir doble factor de autenticación. Tam-

bién puede contar con OTP, aunque haciendo uso de funcionalidad de tercera herramienta, como por ejemplo Yubico OTP. Utiliza cifrado AES 256 de manera local. Permite sincronización de datos entre distintos dispositivos a través de los servidores de Dashlane.

6.4 1Password

1Password fue creado por AgileBits, una empresa privada que desarrolló el software en 2005. Es multiplataforma, siendo posible su funcionamiento para Windows, Mac, iOS y Android. Utiliza cifrado AES256. Cuenta con un buen sistema de clasificación de la información, permitiendo establecer diferentes categorías como inicio de sesión, elemento de cartera, licencia de software, etc. Su sistema de sincronización es sencillo y hace uso de servicios como Dropbox o iCloud. La autenticación se realiza a través de clave maestra e incorpora la posibilidad de autenticación en dos factores. Permite hasta 1GB de almacenamiento.

7 CONCLUSIONES

A lo largo de este documento se ha explicado en qué consisten los Gestores de contraseñas, aplicaciones orientadas a permitir al usuario la administración de sus contraseñas de manera cómoda. El uso de estos gestores se considera una buena práctica de seguridad informática, ya que facilitan la solución al problema de tener demasiadas contraseñas distintas para todos los servicios web que requieren credenciales, situación en la que a menudo el usuario opta por repetir contraseñas, establecer pequeñas variantes de las unas con respecto a las otras o incluso guardarlas todas en un archivo en texto claro, con los riesgos de seguridad que ello conlleva.

Además de su funcionalidad básica como base de datos encriptada de credenciales, se ha podido observar que los gestores de contraseñas cuentan con otros usos avanzados como generar contraseñas aleatorias seguras, creación de grupos de contraseñas, autocompletado de formularios en los sitios web a los que se acceda, etc. Toda esta infraestructura en torno a las credenciales del usuario le permiten al mismo contar con un buen soporte para ganar robustez a la hora de administrar sus contraseñas y en facilidad de uso al tener toda la información accesible en un lugar seguro.

Hay multitud de gestores para elegir, por lo que de manera orientativa se recomienda al usuario que antes de decantarse por uno u otro tenga en cuenta lo siguiente:

- El gestor debe ser sencillo de manejar, si se encuentra demasiado complejo su uso quizá sea más favorable buscar uno que se ajuste al gusto y experiencia de cada uno.

- El gestor debe funcionar en todos los dispositivos desde los que se acceda a las aplicaciones de uso habitual del usuario. También debe presentar la posibilidad de sincronización sencilla entre los distintos dispositivos.

- Es bueno informarse en blogs o portales con buena reputación sobre qué gestores son confiables y seguros. Es importante ver que el gestor ofrece actualizaciones periódicas y que cuenta con diversas opiniones favorables sobre su uso en los foros especializados.

- El gestor debe contar con un buen generador de contraseñas que incluya además un comparador que informe sobre la robustez de las mismas.

- Debe ser posible almacenar más información confidencial además de contraseñas: respuestas a preguntas secretas de seguridad, tarjetas de crédito, códigos PIN, etc.

8 GLOSARIO

Autenticación de dos factores: procedimiento para agregar una capa de seguridad adicional al proceso de inicio de sesión. Cuando el usuario se dispone a iniciar sesión se le solicita que autentifique la titularidad de la cuenta pero proporcionando dos factores distintos. El primero suele ser la contraseña y el segundo puede ser desde un SMS al móvil, una pregunta personal secreta o cualquier otro método de identificación del usuario.

AES (256): esquema de cifrado por bloques adoptado como estándar de cifrado por el gobierno de Estados Unidos. Cuenta con un tamaño de bloque fijo de 128 bits y tamaños de llave de 128, 192 y 256 bits. En el caso particular de los gestores de contraseñas mencionados todos optan por tamaño de llave de 256 bits. Con llaves de longitud alta (192, 256) está considerado un algoritmo muy seguro y aún no hay evidencias de que haya sido vulnerado.

Clave maestra: contraseña única con la que el usuario desbloquea el acceso a su base de datos de credenciales. Dicha base de datos se encuentra cifrada usando la clave maestra.

OTP (One Time Password): contraseñas de un solo uso. Se configura una lista de contraseñas válidas y una vez se produzca el acceso usando una de ellas, esta expirará de la lista y no podrá volver a utilizarse. Es una forma de garantizar la seguridad en el inicio de sesión desde dispositivos que no sean de confianza, evitando la acción de un posible Keylogger. Incluso si la contraseña es comprometida, esta no será válida para futuros accesos.

Red Tor: proyecto cuyo objetivo principal es el desarrollo de una red de comunicaciones distribuida en la que se proteja la identidad del usuario. Persigue que no se puede rastrear la información enviada por un usuario de manera que pueda llegarse hasta él (su dirección IP). Para ello la red Tor cifra la información a la entrada y la descifra a la salida, se basa en lo que se conoce como encaminamiento de cebolla buscando lograr el enrutado anónimo.

TLS: protocolo criptográfico que garantiza una comunicación segura a través de una red, normalmente Internet. Proporciona autenticación y privacidad de la información entre extremos sobre Internet gracias al uso de criptografía. Habitualmente, sólo el servidor es autenticado (es decir, se garantiza su identidad) mientras que el cliente se mantiene sin autenticar.

Twofish: método de criptografía simétrica con cifrado por bloques. Cuenta con un tamaño de bloque de 128 bits y una longitud de clave de hasta 256 bits. Surgió como competencia a AES, aunque en la actualidad este último sigue siendo más usado.

9 DOCUMENTACION DE REFERENCIA

https://www.xataka.com/seguridad/gestores-de-contrasenas-que-son-como-se-usan-y-cual-es-el-mejor
http://www.clavesegura.org
https://en.wikipedia.org/wiki/Password_manager
https://es.wikipedia.org/wiki/Gestor_de_contrase%C3%B1as
https://andro4all.com/2017/03/7-pasos-crear-contrasena-perfecta-segura
http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-sg-es-4/s1-wstation-pass.html
https://password.es/comprobador

https://redminerva.org/gestor-contrasena-internet/

http://blog.elhacker.net/2015/09/diferencias-comparativa-de-gestores-de-contrasenas-passwords-master-windows-linux-android.html

http://computerhoy.com/listas/internet/estos-son-mejores-gestores-contrasenas-64152

https://en.wikipedia.org/wiki/KeePass
https://keepass.info

https://es.wikipedia.org/wiki/LastPass_Password_Manager
https://www.lastpass.com/es

https://en.wikipedia.org/wiki/1Password

https://1password.com

https://en.wikipedia.org/wiki/Dashlane
https://www.dashlane.com/es
https://forums.lastpass.com/viewtopic.php?f=12&t=275575&sid=66f94ad17087f78283eab033db030c8f

https://blog.malwarebytes.com/101/2017/05/dont-need-27-different-passwords

https://blogs.dxc.technology/2017/05/16/gestor-de-contrasenas-herramienta-segura-o-vulnerable

https://solucionindividual.com/solucionindividual/nuestro-blog/entry/gestor-contrasenas.html