PAC1
Gestores de contraseñas

Seguridad informática

Luis Mateo

NIUB 14501432

Sumario

1. Introducción

Los gestores de contraseñas

The Next Domino to Fall: Empirical Analysis of User Passwords across Online Services, es un estudio realizado en 2018 por investigadores de la universidad de Virginia Tech junto con analistas de Daslane, sobre patrones de modificación y reutilización de contraseñas. Analizan una base de datos con 28 millones de usuarios con sus 61 millones de contraseñas y llegan a la conclusión, que el 52% de estos usuarios utilizan la misma contraseña para varios servicios online de los cuales están subscritos. El 38% reutiliza la contraseña para distintos servicios online y el 21% modifica la contraseña ligeramente.

Alarmante es el caso de las plataformas de compras, donde hay información sensible como la dirección física y la tarjeta de crédito. En este caso, 85% de las contraseñas son reutilizadas o levemente modificadas. En el caso de los correos electrónicos es de un 62%. Peor aún es cuando el estudio presenta, que más del 70% de los usuarios siguen utilizando la misma contraseña un año después en varios servicios online, de los cuales, uno de ellos tuvo filtraciones de contraseñas, y más del 40% 3 años después de una filtración.

Como se puede ver en el estudio, muchos usuarios usan por regla general la misma contraseña o varias contraseñas para toda su actividad online (correo electrónico, plataformas audiovisuales, plataformas de juegos, wifi, plataformas de compras…). Cabe entender, que para el usuario resulte la manera más practica y sencilla para poder acceder a sus servicios online, pero está demostrado que no es la práctica más segura. Los expertos en seguridad y las plataformas de servicios online recomiendan que se utilice una contraseña distinta para cada actividad online y evitar contraseñas con caracteres predecibles (qwerty123).

Los gestores de contraseñas son herramientas que permiten almacenar las contraseñas de los usuarios y el uso automatizado de contraseñas. Estas son sus funciones más básicas que se pueden encontrar incorporadas de manera nativa en los diferentes navegadores o sistemas operativos.

Los gestores de contraseñas de terceros, ofrecen funciones más completas. Pueden crear contraseñas aleatorias de alta seguridad, servicios en diferentes plataformas (IOS, Android, Windows, MacOS), sincronizar equipos a través de la nube (móvil, PC, portátil), notificaciones en el caso que se repitan contraseñas o sean compuestas por caracteres

predecibles, incluso rastreo en la Deep web para comprobar si alguna de las contraseñas se ha filtrado.

La gran mayoría de estos gestores son de pago, pero ofrecen una versión gratuita con unas funciones limitadas.

El objetivo de este trabajo es evaluar tres gestores de contraseñas de terceros y seleccionar el más adecuado en el contexto proporcionado en el punto 2.

2. Contexto

El contexto para la evaluación se basa en un usuario universitario entre 20-30 años con conocimientos medios de informática. Tras una vulneración en una cuenta de un servicio online, decide reforzar la seguridad en todas sus actividades online.

Analizando la seguridad de sus cuestas en los servicios online, observa que utiliza en el 70% la misma contraseña que, además, está compuesta por caracteres predecibles, añadiendo que no tiene activado ninguna autentificación de doble factor.

Acabada la revisión de seguridad, el usuario ha reducido el uso de la misma contraseña de un 70% a un 30%, la contraseña está compuesta por una cadena de caracteres más larga y aleatoria y ha activado la autentificación de doble factor.

Para gestionar ese incremento del número de contraseñas y de su complejidad opta por probar tres gestores de contraseñas.

Los requisitos que busca el usuario son:

- Gestor gratuito.
- Con mayores funcionalidades en su versión gratuita.
- Que pueda sincronizarse con otros equipos.
- Interfaz atractiva e intuitiva.

3. Búsqueda y selección

Para encontrar diferentes sugerencias de gestores de contraseñas, se ha optado por buscar información en diferentes blogs y portales de tecnología. En concreto, se ha seleccionado como fuentes VpnMentor y PCworld.

La selección de los gestores se ha basado en la información y en las características que describían estas fuentes, una vez preseleccionados, se ha ampliado la información a través de su página oficial y se ha comprobado la valoración y opiniones que había en la tienda de aplicaciones de Apple, App Store.

Finalmente, los tres gestores de contraseñas seleccionados son los siguientes:

- Keeper
- Dashlane
- Sticky Password

4. Metodología de pruebas

La metodología se basará en la instalación de las 3 aplicaciones de los gestores de contraseñas seleccionadas en el móvil y se probará durante dos días cada una.

Durante esos dos días, se evaluará los siguientes aspectos:

- Cartera digital
- Interfaz cuidada e intuitiva
- Número de funciones adicionales en la versión gratuita
- Servicio en nube
- Sincronización con otros equipos
- Acceso con contraseña biométrica
- Evaluación de contraseñas
- Notas seguras
- Generador de contraseñas
- Encriptación

Entorno de pruebas:

- Móvil: sistema IOS.
- Ordenador: Windows 10.

Los resultados serán presentados en una tabla cuyos aspectos serán valorados de manera textual, acompañado de unas conclusiones.

5. Resultados

	Keeper	Dashlane	Sticky Password
Cartera digital	SI	SI	SI
Servicio en nube	SI (sólo versión premium)	NO	NO
Sincronización con otros equipos en versión gratuita	NO	SI	NO
Acceso con contraseña biométrica	SI	SI	SI
Evaluación de contraseñas	SI	SI	NO
Notas seguras	SI	SI	SI
Generador de contraseñas	NO	SI	NO
Encriptación	AES-256	AES-256	AES-256
Interfaz cuidada e intuitiva	ACEPTABLE	EXCELENTE	MEJORABLE
Número de funciones adicionales en la versión gratuita	4	4	2

6. Conclusiones

Aunque todos ofrezcan el mismo nivel de seguridad y características diferenciadoras, el que mejor se adapta a las necesidades al usuario del contexto, es el gestor de contraseñas de Dashlane. Este gestor en su versión gratuita, es el único que ofrece una sincronización entre equipos. A pesar de no ser en la nube, se sincroniza a través de un código que ofrece la aplicación de móvil, el cual, hay que ponerlo en una web del programa y automáticamente se baja un ejecutable para instalar. Otro factor que sobresale del resto, es una interfaz cuidada y muy intuitiva. A la hora de incorporar las contraseñas de los servicios online, posee un buscador de URL para seleccionar de manera correcta la del servicio online, incorporando un icono de manera automática del servicio online registrado en su caja fuerte, cosa que el resto, no ofrece buscador, ni información visual. Hay que mencionar también, que fue el único en sincronizase con el llavero del sistema IOS, incorporando todas las cuentas introducidas al llavero de Apple.

Otras herramientas que ofrece el gestor de Dashlane en su versión gratuita son:

- Un panel donde puntúa el nivel de seguridad y cuantas contraseñas se han repetido.
- Un generador de contraseñas que ofrece una personalización al usuario, como la longitud de caracteres de la contraseña (de 4 a 40) y la opción de incorporar o no, letras, números y símbolos.
- Escaneo en la bandeja de entrada para numerar cuantas cuentas están creadas bajo un mismo correo electrónico junto con un análisis de seguridad.
- Y sugerencias para alterar y actualizar contraseñas.

Respecto a Kepper, se podría decir que es la segunda opción, a pesar que no tiene para sincronizar con otros equipos en su versión gratuita, ofrece unas funciones interesantes como un chat protegido, sincronización con Watch, un autentificador de doble factor, protección de enlaces favoritos y de archivos. Keeper ofrece funcionalidades que ya las realizan otras aplicaciones (Google Authenticator, y variedades de chats como Signal, recomendada por E. Snowden).

Por los que se refiere a Sticky Password, es el gestor que peor se adapta a las necesidades del usuario. Ofrece una interfaz sobria pero poco intuitiva, apenas ofrece explicaciones de las funcionalidades donde el usuario puede quedarse un momento bloqueado, además, ofrece funcionalidades básicas, como cualquier gestor de

contraseñas nativo del sistema a parte de un navegador seguro integrado en la aplicación y un generador de contraseñas.

Comentado [W1]: Buen trabajo

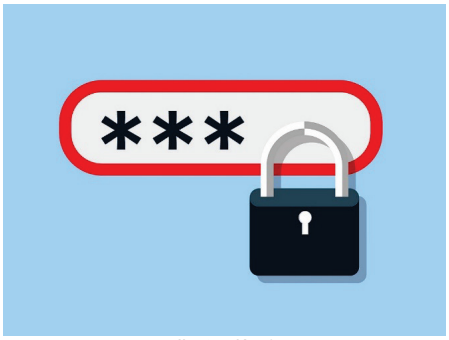

Ilustración 1

7. Valoración de la actividad

Realizar esta actividad me ha ayudado a profundizar más en los gestores de contraseñas, algo que anteriormente había probado por encima. En un principio, comencé a verlo en los navegadores y no me ofrecía mucha confianza. Más adelante, probé con el llavero de contraseñas del sistema IOS, pero tampoco acabé de acomodarme. Ahora que he visto el funcionamiento, sus funcionalidades y su sistema de encriptación y reconozco que es muy práctico y seguro, por lo que me animaré a estar una temporada probándolo.

8. Bibliografía

- El 52% de los usuarios reutiliza sus contraseñas en distintos servicios. (2019). Recuperado 30 Octubre 2019, de https://www.pandasecurity.com/spain/mediacenter/seguridad/reutilizacion-contrasenas/

- El mejor gestor de contraseñas y almacén digital de seguridad | Keeper Security. (2019). Recuperado 30 octubre 2019, de https://keepersecurity.com/es_ES/

- FM, Y. (2019). Gestores de Contraseñas: qué son, cuáles son los más importantes y cómo utilizarlos. Recuperado 30 Octubre 2019, de https://www.xataka.com/basics/gestores-contrasenas-que-cuales-populares-como-utilizarlos

- Hochstadt, A. (2019). Los 10 mejores gestores de contraseñas seguros de 2019. Recuperado 30 octubre 2019, de https://es.vpnmentor.com/blog/los-mejores-gestores-de-contrasenas-seguros-de/

- Mora, A. (2019). ¡Protege tus contraseñas aquí y ahora! Recuperado 30 octubre 2019, de https://www.pcworld.es/mejores-productos/seguridad/gestores-contrasenas-3680297/

- No olvide jamás otra contraseña | Dashlane. (2019). Recuperado 30 octubre 2019, de https://www.dashlane.com/es