Análisis de Seguridad y Uso de Gestores de Contraseñas

Ramirez Leguizamon, Mauricio Andres

2016

Tesis Doctoral 001502/0966

Cod. 1502/0936

Universidad de Buenos Aires

Facultades de Ciencias Económicas, Cs Exactas y Naturales e Ingeniería

Maestría en Seguridad Informática

Tesis

Análisis de Seguridad y Uso de Gestores de Contraseñas

Autor:

ESP. MAURICIO ANDRES RAMIREZ LEGUIZAMON

Directores de Tesis:

Director: **Jacobo Zambrano B.**

Co-Director: **Hugo Pagola**

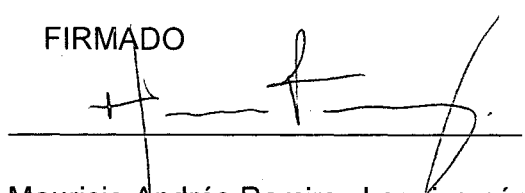
Año 2016

Cohorte 2012

Declaración Jurada de origen de los contenidos

Por medio de la presente, el autor manifiesta conocer y aceptar el Reglamento de Tesis vigente y que se hace responsable que la totalidad de los contenidos del presente documento son originales y de su creación exclusiva, o bien pertenecen a terceros u otras fuentes, que han sido adecuadamente referenciados y cuya inclusión no infringe la legislación Nacional e Internacional de Propiedad Intelectual.

FIRMADO



Mauricio Andrés Ramirez Leguizamón

CC. 80.199.997 Bogotá, Colombia

DNI. 94.761.217 CABA, Argentina

Resumen

Mientras el usuario vaya trabajando con mayor número de servicios que utilicen una identificación de usuario y una contraseña, mayor se vuelve el grado de complejidad existente a la hora de memorizar/administrar dicha información. Debido a lo anterior surgen los gestores de contraseñas, los cuales se encargan de administrar la información de autenticación del usuario y proveen un nivel de seguridad adicional.

El presente trabajo muestra el funcionamiento de diferentes soluciones de gestores de contraseñas en un ambiente de trabajo controlado, exponiendo las características que tiene cada uno para el usuario en aspectos de confidencialidad, integridad, disponibilidad, resguardo de datos, privacidad, auditoria y facilidad de uso. Adicionalmente, se presenta un trabajo de recopilación de información a través de una encuesta que expone quien usa gestores de contraseñas en la actualidad y cuál es el tipo de gestor que utiliza cada grupo de usuarios identificados.

A partir del presente trabajo se establece una métrica para los diferentes tipos de gestores de contraseñas determinando cuál es más seguro, y si es habitual el uso de gestores de contraseñas por las personas, cual es el que mayormente usan y las posibles formas de minimizar las vulnerabilidades detectadas en los gestores analizados.

Palabras clave

Autenticación, usuario, contraseña, vulnerabilidad, gestor de contraseñas.

Índice

Prologo

A Dios Gracias.

Quisiera hacer el reconocimiento de esta obra a las siguientes personas por su amabilidad y apoyo en hacer este trabajo posible:

Mis padres Augusto y Maria, mis hermanos Cesar, Diego y Heidi, y mi primo Omar, porque nada de esto se habría poder realizado sin todos y cada uno de sus aportes.

Un agradecimiento especial a mi tutor Jacobo Zambrano, por todo el acompañamiento recibido en estos años, la atención a mis múltiples consultas y su experticia en el área de seguridad informática.

Agradecimiento al tutor Hugo Pagola, quien me orientó para cerrar aspectos importantes en el desarrollo de esta tesis.

Nómina de abreviaturas y términos

BD: Base de datos

HOTKEYS: Abreviación de teclas

KEYFILE: Archivo llave

KEYLOGGER: Registrador de teclas

MASTER PASSWORD: Contraseña Maestra

OTP: *ONE TIME PASSWORD* (Contraseña de un solo uso)

PASSPHRASE: Frase de contraseña

PIV: Tarjeta de verificación de identificación personal para el control de acceso físico y lógico

SHA: Secure Hash Algorithm

SSO: Single Sign On

I. Introducción

Los gestores de contraseñas se han vuelto cada vez más populares, actualmente se puede encontrar desde utilidades muy elaboradas con muchas funcionalidades que cuentan con el respaldo de publicaciones en revistas que hablan de las bondades y ventajas del producto, así como por otro lado, pequeñas utilidades que sin tener muchas características adicionales, permiten administrar la identificación del usuario y la contraseña de manera sencilla.

En el presente trabajo se pretende mostrar una investigación formal que exponga cual es la tendencia del uso de gestores de contraseñas por parte de usuarios según el universo de gestores de contraseñas existentes (ver Ilustración 1 Universo de Gestores de Contraseñas), y evaluar aspectos de seguridad de los diferentes tipos de gestores de contraseñas, resaltando ventajas y desventajas, debilidades o vulnerabilidades de los sistemas descritos en términos de confidencialidad, disponibilidad e integridad, utilizándolos en un entorno virtual acercando al lector a determinar cuáles serían las posibles soluciones (teóricas) que podrían minimizar el riesgo asociado a seguridad en cada uno y de este modo permitir acercarse a la mejor solución que se adecue a determinado tipo de usuario.

1. Objetivos

General

Determinar qué tipo de gestor de contraseñas ofrece mayores ventajas de seguridad para un usuario en la actualidad.

Específicos

- Describir la forma en que se administra la información del usuario (identificación de usuario y contraseña) de manera general en un gestor de contraseñas.
- Determinar ventajas, desventajas y vulnerabilidades de los distintos tipos de gestores de contraseñas.
- Determinar fortalezas y debilidades en cuanto al uso de los gestores de contraseñas.
- Identificar distintos tipos de usuarios para diferentes gestores de contraseñas en la actualidad.

2. Hipótesis

Preguntas	Objetivos	Hipótesis
¿Cómo funcionan los gestores de contraseñas?	Describir la forma en que se administra la información del usuario (identificación de usuario y contraseña) de manera general en un gestor de contraseñas	El uso de un gestor de contraseñas añade un nivel de seguridad a la administración de contraseñas.
¿Qué diferencia hay entre un gestor de contraseñas y otro?	Determinar ventajas, desventajas y vulnerabilidades de los distintos tipos de gestores de contraseñas.	El uso de un gestor de contraseñas de tipo X trae más ventajas que uno de tipo Y.
¿Es seguro usar un gestor de contraseñas?	Determinar fortalezas y debilidades en cuanto al uso de los gestores de contraseñas.	El uso de los gestores de contraseñas reduce la brecha de seguridad en cuanto a la administración/almacenamiento de los datos de usuario en un sistema.
¿En la actualidad quienes usan los gestores de contraseñas?	Identificar distintos tipos de usuarios para diferentes gestores de contraseñas en la actualidad.	Los gestores de contraseñas son usados tanto por usuarios comunes como por usuarios avanzados.

Tabla 1 Hipótesis

3. Alcance

Actualmente, el mundo se orienta cada vez más hacia el uso de Internet: se leen noticias, se consulta el estado del tiempo, se investigan tareas, se consulta correo, se accede a las redes sociales, se hacen pagos de servicios, se utilizan tarjetas de crédito, etc. Lo anterior implica relacionar información confidencial de un usuario en la web, que no tiene por qué ser visible, ni de fácil acceso a todo el mundo, esto conlleva a generar mecanismos que de algún modo mitiguen las posibles intrusiones y amenazas de seguridad las cuales vulneran el acceso a los servicios del usuario y el posible uso de la información confidencial del mismo.

En este caso, el tema a tratar son los datos de autenticación del usuario, específicamente los nombres de usuarios y las contraseñas; mientras el usuario vaya trabajando con mayor número de servicios que utilicen una identificación de usuario y una contraseña, mayor se vuelve el grado de complejidad existente a la hora de memorizar dicha información.

Con el desarrollo del trabajo se mostrará el funcionamiento de tres de los principales sistemas de gestión de contraseñas en función del almacenamiento de contraseñas (uno por cada tipo de gestor identificado en el Universo de Gestores de Contraseñas) con el fin de determinar los pros y contras de cada uno, notando al final del estudio cuales características son más seguras para su uso y las posibles formas teóricas de solucionar los problemas encontrados. Adicionalmente se mostraran las principales características de funcionamiento de una solución local que utiliza sincronización de datos en la nube.

La encuesta de este trabajo está orientada a cualquier tipo de persona que interactúe con servicios que requieran autenticación a través de Internet; al final del estudio se muestran los resultados correspondientes agrupados por diversas categorías.

Queda por fuera del alcance de este trabajo analizar los algoritmos con que se cifran las BD de los gestores de contraseñas así como la forma en que se generan las contraseñas aleatorias (función presente en algunos gestores de contraseñas).

Los gestores de contraseñas a utilizar serán versiones finales, está por fuera del alcance de este trabajo utilizar versiones beta.

Los gestores a analizar son:

- ***KEEPASS2***: En este estudio se analiza la funcionalidad local de la herramienta.
- ***LastPass***: En este estudio se analiza la funcionalidad online de la herramienta.
- ***Roboform2Go***: En este sentido se analiza la funcionalidad portable de la herramienta instalada en una memoria *USB*.
- ***Dashlane***: En este sentido se analiza la funcionalidad de la herramienta que es local pero que sincroniza los datos en la nube.

II. Levantamiento de Información

1. Justificación de la Encuesta

Se construyó una encuesta sobre la temática (ver Anexo 1 Encuesta sobre uso y conocimiento de Gestores de Contraseñas), con el propósito de determinar cuál es el uso y nivel de apropiación de gestores de contraseñas en la actualidad por diferentes tipos de usuarios. Adicionalmente, a través de esta encuesta se podrá determinar de manera general cuales son las prácticas de habituales de los usuarios para proteger sus contraseñas.

2. Análisis de Resultados

A partir de la encuesta, se lograron identificar dos tipos de usuarios:

1- Comunes y
2- Avanzados

Los resultados en detalle de la encuesta, se muestran en el anexo 1 Encuesta sobre uso y conocimiento de gestores de contraseñas.

Los usuarios comunes son los que tienen un nivel bajo de protección en la administración de sus datos personales debido a que no cumplen con algunas prácticas fundamentales de seguridad (por ejemplo cantidad de caracteres para el armado de las contraseñas o contraseñas de asociación fácil a sus datos personales como DNI y otros), en otras palabras, es el usuario de a pie. Este tipo de usuarios se identificó con los siguientes criterios principalmente:

- Personas que usen más de un servicio que requiera inicio de sesión en internet (99%)
- Que utilicen la misma contraseña para más de un servicio (69%)
- Que alguna vez haya olvidado la contraseña (82%)
- Que las contraseñas que utilicen sean de menor tamaño a 8 caracteres (14%)
- Cambien de contraseña cada vez que el software se lo solicite o nunca cambien de contraseña (51%)
- La forma de administrar las contraseñas sea memorizándolas (64%)

Los usuarios avanzados son los que tienen un nivel de protección mayor en la administración de sus datos personales debido a que combinan varias buenas prácticas de seguridad a la hora de gestionar sus contraseñas.

A continuación, se muestran niveles de seguridad que ayudan a proteger las contraseñas a partir del cumplimiento de las siguientes condiciones:

- Condición 1. Utilizan más de 8 caracteres para generar sus contraseñas (86%)
- Condición 2. Las contraseñas que utilizan, no son de fácil asociación a documentos, email o información dependiente del usuario (88%)
- Condición 3. Utilizan combinaciones de letras con números y caracteres especiales para crear las contraseñas (92%)
- Condición 4. Cuando cambia de contraseña esta difiere de la anterior notoriamente (51%)
- Condición 5. No utiliza la misma contraseña o alguna similar para más de un servicio (31%)
- Condición 6. Cambia sus contraseñas cada 1 a 3 meses (15%)
- Condición 7. Usa una frase de contraseña para definir la contraseña (18%)

El nivel de consciencia en relación al cuidado de los datos es mayor si se combinan las practicas anteriormente mencionadas; es decir, entre más niveles de seguridad se añadan, más segura va a ser la contraseña del usuario. En este sentido, el estudio arrojo los siguientes resultados:

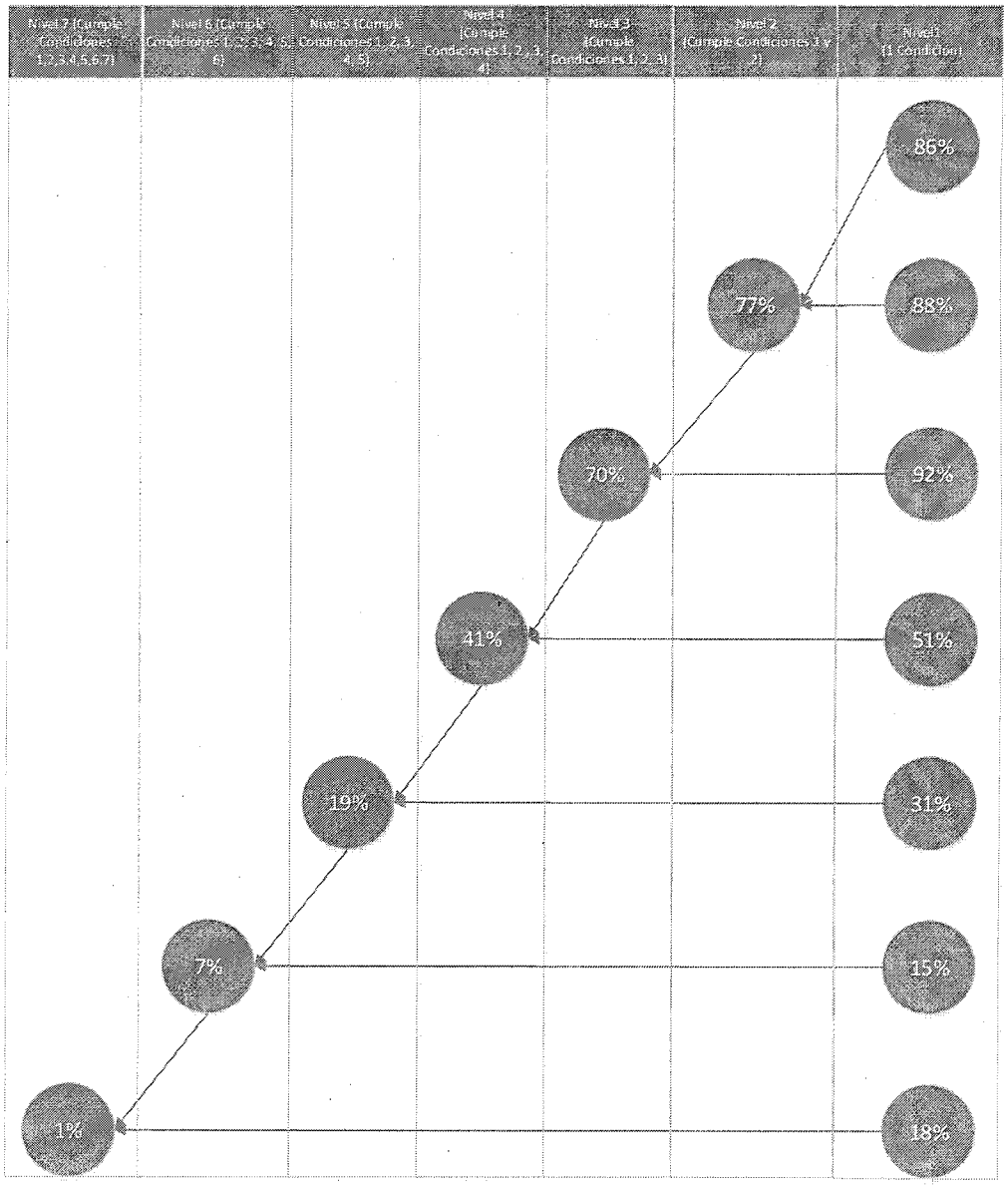


Ilustración 1 Niveles de seguridad según buenas practicas

3. Conclusiones a partir de los Resultados de la encuesta

Las personas cuyo rango de edades va de los 25 a los 40 años constituyen el mayor grupo de personas que accedieron a contestar la encuesta e independiente de su nivel de estudio, sexo o país de residencia, utilizan más de un servicio a través de Internet, donde los más populares son Gmail, Skype y Facebook.

El mayor grupo de personas que respondió la encuesta fueron los Universitarios y los resultados relacionados a estos muestran la problemática existente en cuanto al primer recurso que se utiliza para administrar las contraseñas: la memoria, ya que la totalidad de los encuestados manifestaron alguna vez haber olvidado sus contraseñas.

La mayoría de usuarios son conscientes que tienen falencias a la hora de elegir sus contraseñas, es decir, no confían del todo en las contraseñas que ellos mismos eligieron para cuidar los accesos a sus servicios. Conforme se avanza en los niveles de seguridad que se preguntaban en la encuesta, aumentando las combinaciones de las siete condiciones de seguridad propuestas de buenas prácticas en materia de gestión de contraseñas, se reduce notoriamente la cantidad de personas que utiliza las siete condiciones de seguridad; a partir de lo anterior se puede afirmar que no existe un nivel de conocimiento adecuado en materia de seguridad por parte del grupo de personas encuestadas para administrar sus contraseñas.

La minoría de personas encuestadas utiliza algún sistema de gestión de contraseñas para administrar sus cuentas de usuario, con este estudio se podrá motivar a un usuario que no utiliza un sistema gestor de contraseñas, a utilizar el que más se adecúe a sus necesidades.

La mayoría de las personas encuestadas que utilizan un sistema gestor de contraseñas, confían en mayor grado para delegar sus datos de usuario en la solución local y en menor grado en la solución online.

Los resultados de la encuesta demuestran que la mayoría de personas utilizan más de dos servicios en Internet, lo cual sugiere el uso de un sistema

gestor de contraseñas para que puedan administrar sus contraseñas y datos de usuario de manera adecuada.

Las personas que utilizan los sistemas gestores de contraseñas afirman conocer las características y facilidades de la herramienta que están utilizando pese a no estar satisfechos totalmente por el sistema que eligieron.

Según el estudio, la característica fundamental que manifiestan los usuarios que hace falta para la solución que utilizan, es el acceso a los datos desde cualquier parte, esta característica funciona generalmente en los Gestores de Contraseñas de tipo Online siempre y cuando se tenga acceso al servicio desde internet y a los Portables siempre y cuando se lleve consigo a cualquier sitio el dispositivo donde esta almacenada la información.

La mayoría de las personas encuestadas cambiarían de herramienta a partir del resultado de este estudio. Las personas que NO cambiarían, lo harían debido a que están acostumbradas a la herramienta que utilizan, otro motivo importante es a causa de la desconfianza al momento de cambiar de herramienta y temor al delegar los datos a otra herramienta que no sea la propia.

III. Análisis de Gestores de Contraseñas

Para analizar los gestores de contraseñas se establecieron indicadores para determinar pros y contras de cada una de las herramientas empleadas. Los aspectos evaluados se describen a continuación:

Confidencialidad:

En este contexto, evaluar por cada herramienta: tipo de algoritmo para cifrar los datos, ingreso a la herramienta, generador de contraseñas, protección del ingreso a la herramienta, protección de la memoria RAM y seguridad en el autocompletado.

Integridad:

En este contexto, evaluar por cada herramienta que la BD de contraseñas no pueda ser alterada o modificada.

Disponibilidad:

En este contexto, evaluar por cada herramienta el servicio 7x24 y que se pueda contar con los datos cuando sea que se necesiten.

Resguardo de datos:

En este contexto, evaluar por cada herramienta la posibilidad de realizar copia de seguridad de los datos de usuario y si está protegida dicha copia.

Privacidad:

En este contexto, evaluar por cada herramienta si ofrecen autocompletado y la posibilidad de autenticación de doble factor.

Auditoria:

En este contexto, evaluar por cada herramienta la posibilidad de realizar trazabilidad a las acciones hechas en la herramienta como inicios de sesión y modificación del almacén de datos.

Facilidades de uso:

En este contexto, evaluar por cada herramienta la sencillez de uso, idiomas, plataformas e integración con navegadores, y si cuentan con un medidor de calidad de contraseñas.

Por cada una de las categorías mencionadas anteriormente, se obtuvo una calificación de 0 a 3, siendo 0 la menor opción y 3 la opción de mayor peso. La calificación por ítem está dispuesta en función del análisis de cada opción representada.

Detalles de instalación y prestaciones de los Gestores de Contraseñas expuestos se encuentran en el Anexo II Instalación y prestaciones de los Gestores de Contraseñas analizados.

1. Almacenamiento de datos en Gestores de Contraseñas

Una contraseña es una cadena de caracteres (numéricos, alfabéticos o signos) secreta que es usada para probar la identidad de un usuario en el proceso de autenticación ante un sistema o para acceder a un recurso específico. Las contraseñas existen desde la antigüedad y se ha hecho más recurrente su uso conforme va evolucionando el hombre. El origen de las contraseñas se da con los "santo y seña" que eran utilizados por las legiones romanas para dar accesos a lugares específicos, el mecanismo de funcionamiento era: llegando al lugar requerido, se le preguntaba al visitante el santo y seña y posteriormente, si era correcto, se le permitía acceso al lugar físico al visitante, de lo contrario se le negaba.

A través del tiempo el uso de contraseñas ha evolucionado más que todo en la forma de implementación. Así pues se pueden ver ejemplos como el *ONE TIME PASSWORD* (OTP)[1], el cual es un método en el cual, cada contraseña es válida para una única sesión y por otro lado está la implementación de la combinación de más de un factor de autenticación [1]. El solo uso de una contraseña para autenticarse ante un sistema per se es visto como un sistema de autenticación débil, mientras que la combinación de

[1] OTP: Contraseña de un solo uso

contraseña con otros factores de autenticación como huella digital, permiten establecer un sistema de autenticación fuerte que va a ser menos vulnerable.

Las políticas basadas en contraseñas para el control de accesos son la solución más habitual; sin embargo este método presenta varios inconvenientes:

- La contraseña generada puede dejarse anotada en cualquier parte o puede usarse una contraseña fácil de descubrir.
- En los sistemas donde la política de contraseñas es más rigurosa, se obliga al usuario a manejar secuencias de caracteres complicadas que tienen que cambiarse periódicamente y perjudican al usuario al tener que memorizarlas de nuevo cada cierto tiempo.
- El perder u olvidar la contraseña, aparte de ser un problema para el usuario, supone costos adicionales de administración en una organización. Por ejemplo, esto supone gastos en lo que conlleva la gestión de un incidente a través de la mesa de ayuda y el tiempo de no productividad del usuario hasta que se le resuelva el incidente.
- La existencia de malware como por ejemplo un *KEYLOGGER*[2] puede capturar la contraseña del usuario abriendo la posibilidad de suplantación del usuario o de adquirir información de la cuenta afectada.

Buenas Prácticas para Generación de Contraseñas

Las contraseñas pueden considerarse como un elemento fundamental en el acceso a un sistema, una contraseña mal creada puede redundar en: robo de información, daño de reputación o responsabilidad legal ante terceros, entre otros, por uso indebido de alguien no autorizado que se haya hecho con la contraseña del usuario. Actualmente no se deberían admitir contraseñas que solo usen las letras del alfabeto debido a que con el cálculo de computo actual, un ataque de fuerza bruta podría descubrir fácilmente estos datos, la

[2] KEYLOGGER: Registrador de teclas

cantidad de posibles contraseñas a partir del alfabeto se muestra a continuación [2]:

Longitud de Contraseña	Potenciales Contraseñas
1	26
2	676
3	17,576
4	456,976
5	11,881,376
6	308,915,776

Tabla 2 Cantidad de Combinaciones a partir de alfabeto

Las buenas prácticas mencionan algunas de las siguientes características para tener una contraseña segura [3][4][5][6]:

1. Utilizar contraseñas complejas y únicas para cada cuenta, como la combinación letras, números y signos
2. Tener 8 caracteres de longitud como mínimo
3. Evitar que sea de fácil asociación de datos dependientes del usuario (Ejemplo: DNI, nombre, teléfono)
4. Cambiarla frecuentemente en función del servicio utilizado (es distinta la importancia de los servicios que se utilizan, por ejemplo: la cuenta de un buscador de empleo en relación a la cuenta bancaria)
5. Que la contraseña nueva difiera de la anterior, y que no se reutilicen las contraseñas
6. Usar un *PASSPHRASE*[3] para definir la contraseña

[3] PASSPHRASE: Frase de Contraseña

Aparte de lo anterior, es muy recomendable mantenerse en sitios de confianza, por ejemplo, si se tiene una lista de sitios web que son visitados con frecuencia y en los que se confía plenamente, se pueden agregar a la zona de sitios de confianza del navegador, esto minimizara la posibilidad de navegar por sitios falsos que se asemejan a los reales donde se tiene algún servicio.

Todo lo anterior resuelve de algún modo la problemática en la cual la contraseña se hace más difícil de averiguar o predecir, sin embargo no resuelve el problema de administrar muchas contraseñas diferentes para distintos servicios complicando el cumplir con las buenas prácticas mencionadas anteriormente para cada servicio que se tenga.

A medida que va creciendo la demanda por usar servicios virtuales (aplicaciones, redes sociales, correo, banca, servicios varios), se van generando otras variables que de una u otra forma repercuten en las actividades que implican el registro de un usuario ante un sistema, mientras el usuario vaya trabajando con mayor número de servicios que utilicen una identificación de usuario y una contraseña, mayor se vuelve el grado de complejidad existente a la hora de memorizar/administrar dicha información. Por lo anterior es recomendable implementar alguna solución que administre los datos de autenticación y sea confiable para el usuario, en este sentido, para los servicios que requieren registro de usuario y contraseña (por ejemplo servicios de correo electrónico, redes sociales, etc), existen soluciones de tipo local y en la nube, los cuales consisten en el almacenamiento de estos datos para hacer más segura y fácil la experiencia de navegación del usuario final.

En la actualidad existen diversas soluciones (por ejemplo: *KeePass, ROBOFORM, 1PASSWORD, DASHLANE, PASSWORDSAFE*... etc) que ofrecen en mayor o menor medida un nivel de seguridad, y que a su vez ofrecen distintos tipos de soluciones ya sean locales, portable u online, para que el usuario administre sus datos de usuario y de este modo deje de un lado el problema que conlleva el memorizar numerosas contraseñas.

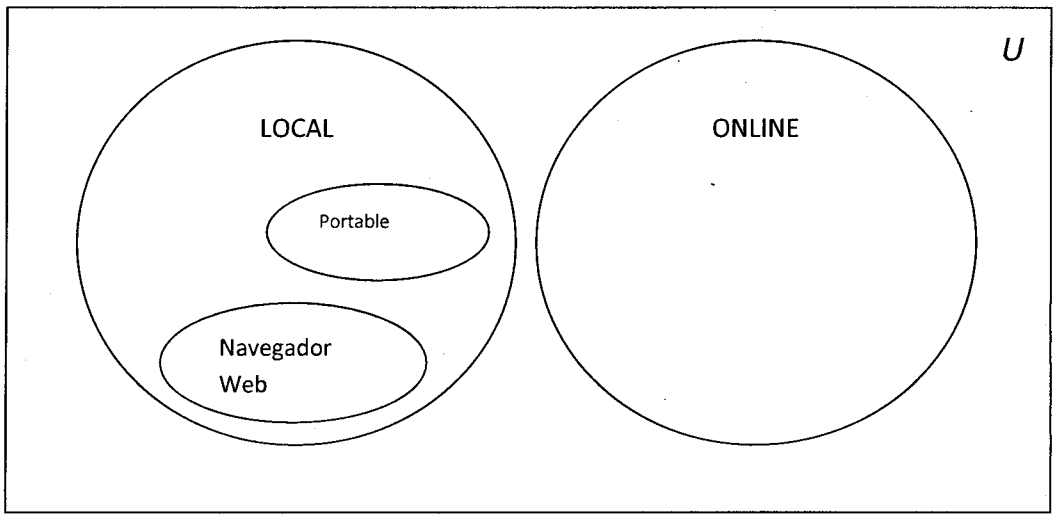


Ilustración 2 Universo de Gestores de Contraseñas

En cada tipo de gestor de contraseñas [7] se encuentran diferentes vulnerabilidades en relación a los datos de usuario que se ingresan:

- Mecanismo de funcionamiento: Acceso a la herramienta así como la forma en que se protege la información.
- Lugar de almacenamiento: En donde se guardan los datos obtenidos (Ejemplo: local o en la nube).
- Canal de transferencia: la forma como se transfieren los datos que el usuario ingresa a la base de datos de la herramienta (Ejemplo: a la nube de forma segura o si los datos al ser usados se borran de la memoria en el caso de uso local).

La inseguridad de los gestores de contraseñas se manifiesta al vulnerar uno o varios de los ítems anteriormente contemplados debido a que al quedar comprometidos alguno de los factores anteriores, redundará en conocer los datos de usuario y posteriormente usarlos, sea cual sea el tipo de gestor de contraseña.

En la vida cotidiana se manejan gran cantidad de contraseñas diferentes para servicios que van desde el correo electrónico hasta los datos bancarios, con este gran número de contraseñas el olvido de ellas es común, especialmente si se construyó una contraseña compleja. En algunos casos, la solución que encuentran los usuarios es tener las contraseñas escritas, pero esto supone una práctica riesgosa para la seguridad por ejemplo si

alguien no autorizado tuviera acceso a estos datos, es en este punto donde los gestores de contraseñas juegan un papel importante al día de hoy, para ayudar a resolver este tipo de inconvenientes.

En este trabajo se tratan tres de los gestores de contraseñas más populares en el mercado usados de forma: local, online y portable (en una memoria *USB*), adicionalmente se aborda el análisis de una solución local adicional que sincroniza los datos en la nube. Una situación común para decidir utilizar un gestor de contraseñas es cuando se está navegando y se escribe una contraseña en un formulario y el navegador ofrece recordarla, estando en el computador, ya sea el de la oficina, el de la casa o el de un sitio desconocido. En un trabajo anterior de autoría propia acerca de los gestores de contraseñas en los Navegadores Web, se comentaba que un usuario que usa frecuentemente un computador y que desconoce los riesgos asociados de almacenamiento de datos por un software, acepta la opción de recordar contraseñas en el navegador por comodidad y estos datos son almacenados para la próxima vez que se desee acceder a la misma página; sin embargo surge el problema de si alguien más accede a la sesión del usuario y utiliza por ejemplo el navegador donde se almacenaron los datos pudiendo utilizarlos y aún más, teniendo la posibilidad de conocer cuáles son las contraseñas [8].

El utilizar un Sistema Gestor de Contraseñas añade una capa de seguridad al usuario que quiere proteger sobre todo la confidencialidad de sus datos de inicio de sesión ante un servicio y brinda una administración segura de los datos de autenticación a los servicios. El correcto uso de un Gestor de Contraseñas, reduce la probabilidad de *PHISHING* de acuerdo a la asociación que se hace de los datos del usuario con la página web real del servicio al que requiere acceder el usuario, sin embargo, como se ve en el caso de los Gestores de Contraseñas por Navegadores Web, se potencian los ataques a través de malware para poder obtener los datos de usuario almacenados. Los Gestores de Contraseña analizados en este trabajo ofrecen ventajas sobre los que vienen con los navegadores web debido a que tienen más características de seguridad implementadas, por ejemplo contra ataques de fuerza bruta y otras características que se describen en el siguiente capítulo.

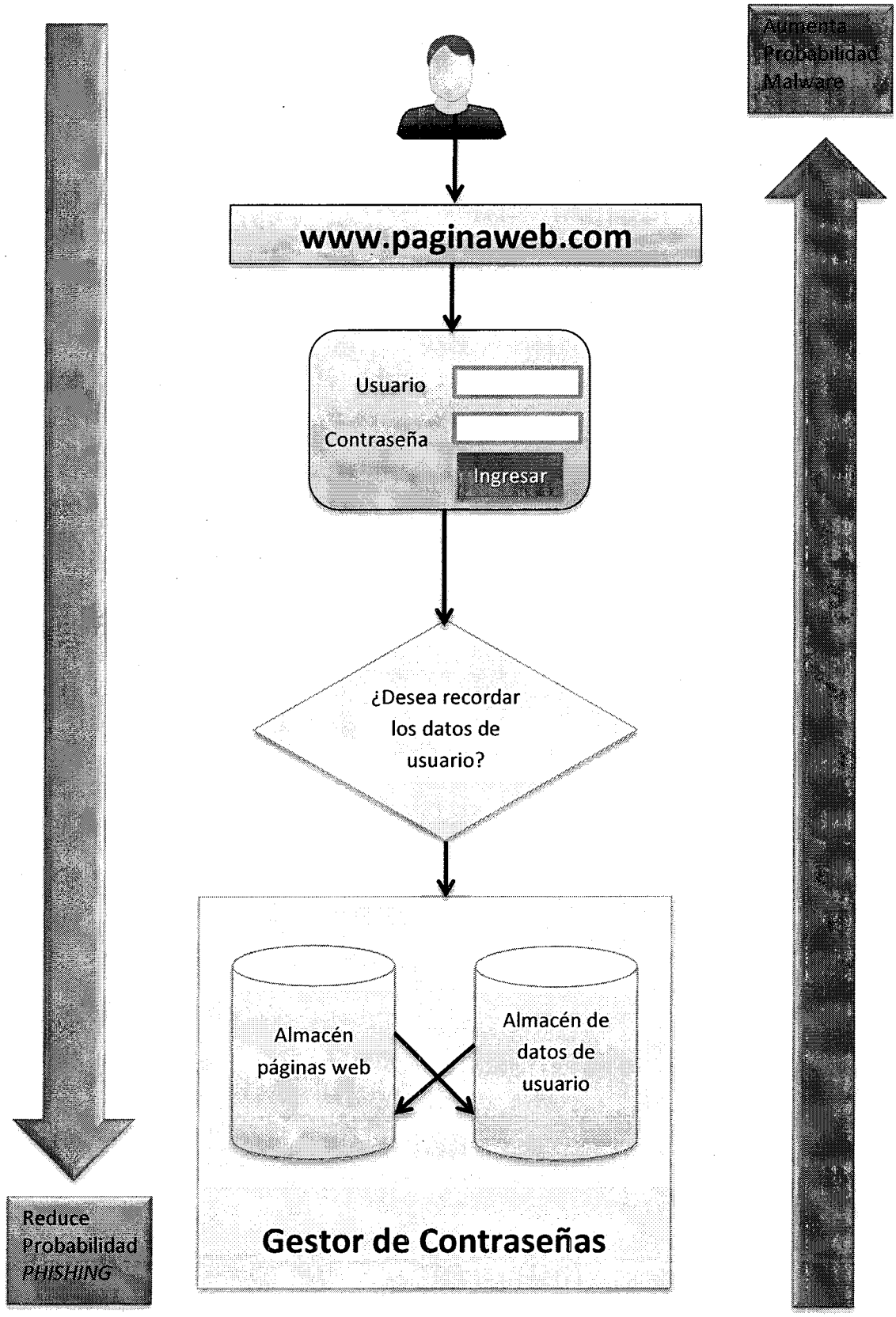


Ilustración 3 Gestión de datos de usuario

2. Comparación técnica de los Sistemas Gestores de Contraseña analizados

A continuación se resumen las principales características que a consideración para este estudio, son las más relevantes en la comparación de los Gestores de Contraseñas analizados:

2.1 Compatibilidad de plataformas

Una aplicación multiplataforma es un atributo concedido a software que es implementado e inter-opera entre múltiples plataformas informáticas. Esta característica se considera importante debido a que contribuye a la facilidad que tiene un usuario que utiliza cierta plataforma o diferentes plataformas a la vez.

KeePass v.2.28

Es Multiplataforma.

Funciona en *Linux*, *Windows*, MacOS y BSD. Existen las siguientes versiones: *KeePass* X *Linux*, Macos, 7pass winphone, *KeePass* for Blackberry, *KeePass* Mobile (Java ME) *KeePass* for J2ME, i*KEEPASS* para iphone, *KEEPASS*droid para Android y *KeePass* para dispositivos inteligentes con *Windows* Mobile y pocket PC.

LastPass v.3.1.65

Es Multiplataforma.

Funciona desde cualquier sistema operativo accediendo directamente a la página web en la página web https://*LastPass*.com (después de haberse registrado); adicionalmente se puede instalar un *PLUGIN* para los navegadores *IEXPLORER*, *FIREFOX*, chrome, opera y safari.

La versión paga (Premium) es para Iphone, BlackBerry, Android, winphone, winmobile, webos, y symbian.

Roboform2Go v.7.9.9.1

No es Multiplataforma.

Roboform2Go es la versión para memoria *USB* de la herramienta *ROBOFORM*. *Roboform2Go* es solo para *Windows* y funciona solamente con los navegadores *IEXPLORER* y *FIREFOX*

Dashlane 4.1.1.10306

Es Multiplataforma aunque limitado a sistemas operativos. Funciona en Mac, Windows, Android, IOS.

No funciona en Linux, Windows Mobile, Windows RT, Blackberry, Amazon Kindle ni Chromebook.

Requiere instalación local para poder registrarse como usuario de Dashlane. Adicionalmente se puede añadir como extensión a navegadores, aunque tiene problemas de compatibilidad con Internet Explorer.

2.2 Compatibilidad de Idiomas

Es la característica en la cual la aplicación está disponible para diferentes idiomas.

KeePass v.2.28

Incorpora múltiples idiomas.

LastPass v.3.1.65

Incorpora múltiples idiomas.

Roboform2Go v.7.9.9.1

Incorpora múltiples idiomas.

Dashlane 4.1.1.10306

Incorpora múltiples idiomas.

2.3 Tipo de licencia

Es la característica que determina el contrato que concede la propiedad intelectual y derechos de autor en la cual están precisados los derechos y deberes entre el desarrollador y el comprador en términos de software.

KeePass v.2.28

El tipo de licencia es GPL y el código fuente es en .Net la versión 2.x

LastPass v.3.1.65

El tipo de licencia es Propietario y no hay información disponible sobre su código fuente.

Roboform2Go v.7.9.9.1

El tipo de licencia es Propietario y no hay información disponible sobre su código fuente.

Dashlane 4.1.1.10306

El tipo de licencia es Propietario y no hay información disponible sobre su código fuente.

2.4 Ingreso a la herramienta

Es la característica que describe la forma de acceso a la herramienta.

KeePass v.2.28

Principalmente a través de *MASTER PASSWORD*. El *MASTER PASSWORD* tiene tiempo de caducidad.

Adicionalmente puede utilizar doble factor de autenticación utilizando un KEYFILE que se usa en combinación con el *MASTER PASSWORD* definido para abrir la BD donde se almacenan las contraseñas. Para que sea exitosa la autenticación se requiere que siempre se transporten en conjunto la BD y el KEYFILE. Por otra parte existe la posibilidad de asociar la cuenta de usuario de *Windows* para que de esta forma en combinación con el *MASTER PASSWORD* se pueda acceder a los datos de usuario.

El KEYFILE es un archivo que se genera a partir de la recolección de datos aleatorios. Los datos se recolectan a partir del movimiento del mouse en una zona determinada de la pantalla y a partir del ingreso de caracteres en una caja de texto. Con esta información se genera una semilla para crear una serie criptográficamente fuerte.

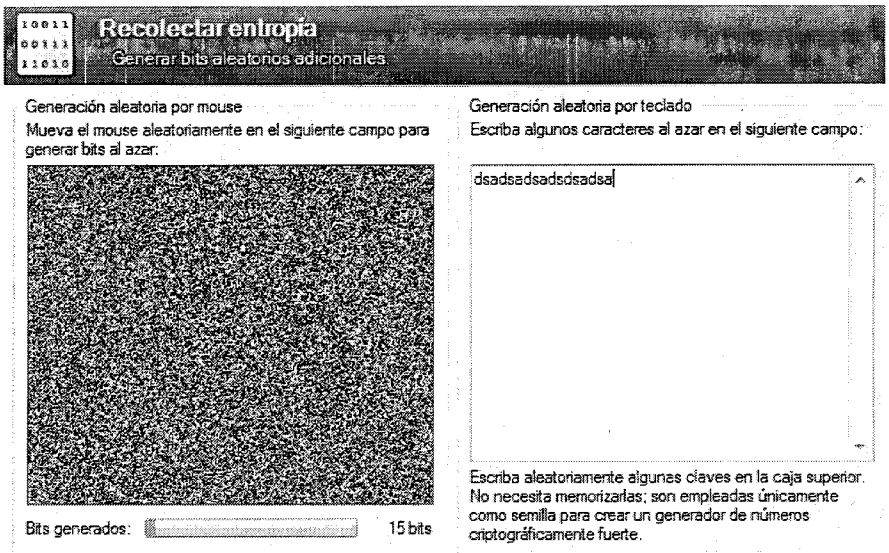


Ilustración 4 Recolección entropía

LastPass v.3.1.65

Principalmente a través de *MASTER PASSWORD*. El *MASTER PASSWORD* tiene tiempo de caducidad.

Adicionalmente puede utilizar doble factor de autenticación a través de diferentes opciones entre las que se encuentran tarjeta de coordenadas, biometría, yubikey, google y otras (la verificación de huella dactilar funciona desde win7 en adelante)

Una ventaja importante de *LastPass* es que ofrece la posibilidad de generar contraseñas de un solo uso (OTP). Si se usa un computador público que no es de confianza por ejemplo donde se sospeche que tiene un KEYLOGGER instalado, y se requiere acceder a los datos en *LastPass*, la herramienta ofrece *ONE TIME PASSWORD*s (OTP) como una opción para acceder de forma segura a la cuenta.

Para usar esta característica, es necesario acceder previamente desde un equipo que sea de confianza al sitio oficial de *LastPass* en la web y en la sección de herramientas avanzadas, seleccionar Contraseñas de un Solo Uso para crear un listado de contraseñas aleatorias que se podrán utilizar solo una vez para iniciar sesión en *LastPass*. Desde esta sección se podrán agregar OTPs al listado, borrar todo el listado, o imprimir el listado que se haya generado:

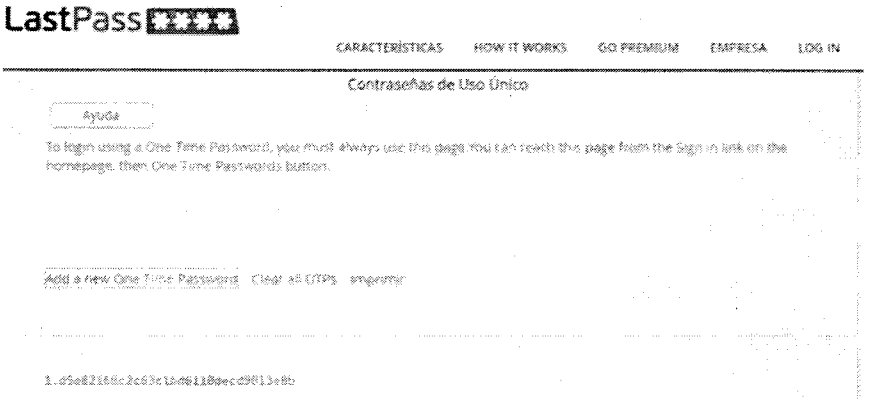


Ilustración 5 *LastPass* OTP

Cada vez que se use una contraseña del listado, el servidor de *LastPass* dará por expirado su uso y la borrara de almacén de contraseñas de ingreso a la herramienta para que cuando se quiera usar de nuevo la contraseña, esta no funcione.

La opción de OTP se puede combinar con otra forma de autenticación para hacer más seguro el ingreso a los datos, cuando no se esté usando un equipo de confianza.

Roboform2Go v.7.9.9.1

Principalmente a través de *MASTER PASSWORD*.

Adicionalmente puede utilizar doble factor de autenticación a través de biometría (huellas dactilares) y PIV tarjetas inteligentes.

Dashlane 4.1.1.10306

Principalmente a través de *MASTER PASSWORD*.

Adicionalmente puede utilizar doble factor de autenticación con FIDO Alliance, asociado con YUBICO (compañía que provee las U2F de yubikey). Puede instalarse una aplicación adicional de doble factor de autenticación para facilitar el vínculo entre el dispositivo móvil y el acceso a la cuenta de Dashlane a través de un código de seguridad.

También puede utilizar OTP pero a través de funcionalidad de tercera herramienta, por ejemplo Yubico OTP.

2.5 Algoritmo Criptográfico

Es la característica que describe el algoritmo criptográfico con el cual se cifran las BDs que contienen los datos de usuario.

KeePass v.2.28

Utiliza AES, desde la versión *KEEPASS*2.XX no utiliza Twofish.

LastPass v.3.1.65

Utiliza AES 256 localmente antes de ser enviado a *LastPass* a través de SSL.

Roboform2Go v.7.9.9.1

Utiliza Blowfish o AES.

Dashlane 4.1.1.10306

Utiliza AES 256 localmente.

2.6 Portabilidad de datos

Es la característica que describe la factibilidad de transportar los datos almacenados en la herramienta correspondiente.

KeePass v.2.28

La BD puede ser transportada de un computador a otro; sin embargo si fue generado el KEYFILE, este tendrá que ser transportado junto a la BD para que se pueda abrir.

LastPass v.3.1.65

Los datos están en la nube por lo que lo único que se requiere recordar es el *MASTER PASSWORD* para acceder desde cualquier sitio con conexión a internet. Si no se dispone de conexión a internet, no se puede acceder a los datos.

Roboform2Go v.7.9.9.1

El sistema completo (software y datos de usuario) es portable en una memoria *USB*.

Dashlane 4.1.1.10306

Los datos se almacenan localmente en el dispositivo que se esté usando sincronizando con servidores de dashlane (si tiene activa la opción de sincronización), se pueden editar desde la aplicación local y se pueden ver como solo lectura desde la aplicación web.

2.7 Sincronización de datos

Es la característica que describe la forma en la cual se sincronizan los datos de usuario en la herramienta. Esta característica es útil sobre todo, si se maneja desde diversos dispositivos la herramienta y por ejemplo se cambia la contraseña de un servicio desde uno de estos.

KeePass v.2.28

Se puede sincronizar a través de un servidor FTP.

LastPass v.3.1.65

Las BDs se sincronizan en la nube a través de cualquier navegador.

Roboform2Go v.7.9.9.1

Se puede elegir si se sincroniza en la nube con *ROBOFORM* everywhere (versión paga) o si solo se va a usar localmente.

Dashlane 4.1.1.10306

Sincroniza con servidores de Dashlane la info que tiene guardada en el dispositivo que se esté utilizando.

2.8 Generador de contraseñas

Es la característica que describe si la herramienta tiene la facultad de generar contraseñas. Esta característica es útil sobre todo si existe un usuario que desee usar contraseñas robustas para sus servicios pero desconoce las buenas prácticas de seguridad para crear contraseñas.

KeePass v.2.28

La herramienta puede generar contraseñas para los servicios que se quieren administrar a través de la herramienta.

El generador de contraseñas ofrece diferentes opciones para generar la contraseña:

- A través de un conjunto de Caracteres: incluyendo longitud de caracteres, letras mayúsculas y minúsculas, números, caracteres especiales y algún carácter especial que se desee, entre otros.
- A través de un patrón: por ejemplo determinando el conjunto de las vocales [aeiou], se puede generar una contraseña

Dependiendo de la combinación anterior la herramienta generará una fortaleza en bits aproximada la cual será mayor entre más características se combinen.

LastPass v.3.1.65

La herramienta puede generar contraseñas seguras para los servicios que se quieren administrar a través de la herramienta.

El generador de contraseñas crea la contraseña en el equipo del usuario a través de JavaScript, esto quiere decir que la herramienta no va a tener acceso a las contraseñas que el usuario genere. Se puede elegir la configuración con la cual se va a generar la contraseña para el servicio determinado a través de un conjunto de caracteres: longitud de contraseña, letras mayúsculas, letras minúsculas, números, evitar caracteres repetidos, y que requiera cada tipo de carácter de los anteriormente mencionados.

Roboform2Go v.7.9.9.1

Si puede generar contraseñas para los servicios que se quieren administrar a través de la herramienta.

Se puede elegir la configuración con la cual se va a generar la contraseña para el servicio determinado a través de un conjunto de caracteres: número de caracteres, exclusión de caracteres similares, caracteres hexadecimales, letras mayúsculas, letras minúsculas, números y caracteres especiales; dependiendo de la combinación anterior la herramienta generará una fortaleza en bits aproximada la cual será mayor entre más características se combinen.

Dashlane 4.1.1.10306

La herramienta puede generar contraseñas para los servicios que se quieren administrar a través de la herramienta.

El generador de contraseñas ofrece diferentes opciones para generar la contraseña:

- Incluyendo dígitos, letras, símbolos y la opción de que la contraseña pueda ser pronunciable.

2.9 Medidor de calidad de contraseñas

Es la característica que indica si la contraseña que el usuario ingresa es más o menos robusta.

KeePass v.2.28

Si incluye medidor de calidad de contraseñas para *MASTER PASSWORD* y para contraseñas de servicios. Además muestra la calidad estimada en bits del *MASTER PASSWORD*.

LastPass v.3.1.65

Si incluye medidor de calidad de contraseñas para *MASTER PASSWORD* y para contraseñas de servicios.

La herramienta permite también analizar las contraseñas para buscar las debilidades. Por ejemplo advierte de las contraseñas débiles y las que se han utilizado varias veces cuando se conecta a los servicios.

Roboform2Go v.7.9.9.1

Si incluye medidor de calidad de contraseñas para *MASTER PASSWORD*.

Dashlane 4.1.1.10306

Si incluye medidor de calidad de contraseñas para *MASTER PASSWORD* y para contraseñas de servicios.

2.10 Importación y Exportación de datos

Es la característica que indica si se pueden exportar e importar los datos de usuario almacenados en determinada herramienta.

KeePass v.2.28

La herramienta permite importar y exportar datos de usuario.

Se permiten importar datos de los siguientes formatos/aplicaciones:

- *KeePass*:
- *KeePass* KDB (1.x)
- *KeePass* KDB (2.x)
- *KeePass* KDB (2.x) Modo de Reparación
- *KeePass* XML (1.x)
- *KeePass* XML (2.x)
- General:
- Importador CSV generic
- Gestores de Contraseñas:
- 1PW & 1 PasswordPro CSV
- Alle meine Passworte XML
- Any Password CSV
- Code Wallet TXT
- Dashlane CSV
- Data Vault CSV
- DesktopKnox XML
- FlexWallet XML
- Handy Safe TXT
- Handy Safe Pro XML
- Kaspersky Password Manager XML
- *KEEPASSX* XML
- *LastPass* CSV
- Network Password Manager CSV
- Norton Identity Manager CSV
- PassKeeper
- PASSPHRASE Keeper HTML
- Password Agent XML
- Password Depot XML
- Password Keeper CSV
- Password Memory 2008 XML
- Password Prompter DAT
- Password Safe XML
- Passwords Plus CSV
- Passwort. Tresor XML
- Personal Vault TXT
- PINs TXT
- Revelation XML

- Robo Form HTML (Logins/PassCards)
- SafeWallet XML
- Security TXT
- SplashID CSV
- Steganos Password Manager 2007
- Sticky Password XML
- TurboPasswords CSV
- VisKeeper TXT
- Whisper 32 CSV
- ZDNet´s Password Pro TXT
- Navegador:
- Mozilla Bookmarks HTML
- Mozilla Bookmarks JSON
- Password Exporter XML
- Sitios Web:
- Spamex.com

Se permiten exportar datos a los siguientes formatos/aplicaciones:

- *KeePass*:
- *KeePass* CSV (1.x)
- *KeePass* KDB (1.x)
- *KeePass* KDBX (2.x)
- *KeePass* XML (2.x)
- General:
- Archivo HTML personalizable
- Transformador usando una plantilla XSL
- Favoritos de *Windows* (Carpeta *KeePass*)
- Favoritos de *Windows* (Directorio raiz)

LastPass v.3.1.65

Si permite importar y exportar datos de usuario.

Se permiten importar datos de los siguientes formatos/aplicaciones:

- Internet Explorer Password Manager
- *FIREFOX* Password Manager
- Chrome Password Manager
- Safari Password Manager
- Opera Password Manager
- 1Password
- Clipperz

- Darn! Passwords!
- Dashlane
- Ewallet
- Figaro Password Manager
- Fireform
- HP Password Safe
- *KeePass*
- *LastPass*
- McAfee Safekey
- MSI PasswordKeeper
- My PasswordSafe
- Passpack
- Password Agent
- Password Corral
- Password Depot
- Paswword Dragon
- Password Keeper
- Password Safe
- Password Max
- PasswordVault
- PINS Password Manager
- Revelation Password Manager
- *ROBOFORM*
- SafeWallet
- Secret Server
- SPB Wallet
- SplashIS
- Sticky Password
- Sxipper
- TurboPasswords
- Archivo CSV generico

Se permiten exportar datos a los siguientes formatos/aplicaciones:

- Archivo CSV *LastPass*

Roboform2Go v.7.9.9.1

Solo se permiten importar datos de los siguientes formatos/aplicaciones:

- Navegadores:
- *FIREFOX*

- Opera
- Internet Explorer
- Google Chrome
- Aplicaciones:
- Outlook
- Libreta direcciones *Windows*
- Xmarks
- Marcadores en format HTML
- Archivo CSV de *LastPass*
- Archivo CSV de *KeePass*
- Archivo NIS CSV
- Archivo texto 1 Password
- Archivo SplashID CSV

Dashlane 4.1.1.10306

Si permite importar y exportar datos aunque con algunas restricciones.

Importación

Permite importar datos desde CSV o navegadores y desde los sistemas gestores de contraseñas: KeePass,1Password, RoboForm, LastPass, PasswordWallet

No permite importación de datos de IOS y Android.

Exportación

Permite exportar datos en xls o csv

Adicionalmente es la única herramienta que permite la exportación segura de los datos en un archivo seguro de Dashlane (formato de archivo .DASH) el cual podrá ser importado en otra máquina siempre y cuando se tenga instalado Dashlane.

2.11 Ingreso de datos para usar un servicio

Esta característica describe la forma en la que la herramienta ingresa los datos al formulario que contiene los campos de usuario y contraseña requeridos. Generalmente existen dos formas de ingresar los datos: manualmente, haciendo uso de la copia del portapapeles o de automáticamente con la función de autocompletado que ofrecen las herramientas.

El ingreso de datos de usuario es importante en términos de confidencialidad ya que si se utiliza una forma adecuada de ingreso de datos de la herramienta al servicio, se reducirán problemas de seguridad como el *PHISHING*. Un correcto uso de un gestor de contraseñas reducirá el riesgo de un ataque de *PHISHING* debido a que al guardar los datos de usuario, la herramienta asocia estos con el enlace verdadero (siempre y cuando se tenga certeza que el link es verdadero verificando los certificados de seguridad de la página) haciendo que el usuario no entre a buscar la página web manualmente y encuentre una parecida donde quiera cargar sus datos.

KeePass v.2.28

Los datos se pueden ingresar al formulario a través de distintas formas:

- copia del portapapeles desde la herramienta
- arrastrando de la herramienta y soltando la información en los campos requeridos
- autocompletado del formulario mediante configuración de la opción de autocompletado para navegadores para asociar el destino de los datos.

Cuando *KeePass* está en uso, los datos de usuario se almacenan cifrados en el proceso de la memoria, es decir, cuando se copia una contraseña al portapapeles, *KeePass* primero descifra el campo de la contraseña, lo copia al portapapeles e inmediatamente lo vuelve a cifrar usando una clave aleatoria.

En el proceso de autocompletado, *KeePass* envía pulsaciones de teclas adicionales junto con la utilización del portapapeles ofreciendo seguridad que permite engañar KEYLOGGERs.

LastPass v.3.1.65

Los datos se pueden ingresar al formulario a través de distintas formas:

- copia del portapapeles desde la herramienta
- arrastrando de la herramienta y soltando la información en los campos requeridos
- autocompletado del formulario al ingresar a la página web requerida ya que esta es almacenada y asociada a los datos de usuario cuando el usuario ingresa sus datos de ingreso al sitio.

Incluye gestión de formulario para completado y entrada a la página o sitio requerido

Roboform2Go v.7.9.9.1

Los datos se pueden ingresar al formulario a través de distintas formas:

- copia del portapapeles desde la herramienta
- arrastrando de la herramienta y soltando la información en los campos requeridos
- con autocompletado del formulario al ingresar a la página web requerida ya que esta es almacenada y asociada a los datos de usuario cuando el usuario ingresa sus datos de ingreso al sitio.

ROBOFORM ofrece la posibilidad de proteger las entradas para que cuando quieran ser vistas, se solicite el *MASTER PASSWORD*.

Cuando se desconecta la *USB* de un host, el software y los datos son borrados del host.

Dashlane 4.1.1.10306

Los datos se pueden ingresar al formulario a través de distintas formas:

- copia del portapapeles desde la herramienta
- autocompletado del formulario al ingresar a la página web requerida ya que esta es almacenada y asociada a los datos de usuario cuando el usuario ingresa sus datos de ingreso al sitio.

2.12 Auditoria de seguridad

Esta característica describe si la herramienta utiliza algún mecanismo que permita registrar la trazabilidad de las acciones en cuanto a su uso y acceso.

KeePass v.2.28

Permite revisar trazabilidad de fecha de creación, modificación, expiración y ultimo acceso a las entradas.

LastPass v.3.1.65

Permite revisar trazabilidad de fecha de creación, modificación, expiración y ultimo acceso a las entradas.

Roboform2Go v.7.9.9.1

No cuenta con esta característica.

Dashlane 4.1.1.10306

Únicamente cuenta con función de historial de contraseñas anteriores.

2.13 Desventajas

En este punto se describen las principales desventajas detectadas de cada gestor de contraseñas.

KeePass v.2.28

La solución local genera una BD que se utiliza principalmente en el computador donde fue instalada la aplicación, lo cual la hace difícilmente portable si por ejemplo se asocia el *MASTER PASSWORD* con la cuenta de *Windows*.

La sincronización de forma online no es sencilla, tiene aspectos de configuración de servidor FTP que no es entendible para todo tipo de usuario

Al ser escrito en código abierto, *KeePass* compromete la seguridad de la aplicación al dejar que se le puedan añadir *PLUGIN*s que no son verificados.

Soporte principalmente en inglés

LastPass v.3.1.65

Datos de usuario en manos de un tercero (cifrados alojados en los servidores de *LastPass*)

Soporte principalmente en inglés

Si no se dispone de conexión a internet, no se puede acceder al almacén de datos a menos que se instale *LastPass* pocket o *LastPass* Portatil.

Roboform2Go v.7.9.9.1

La versión utilizada en este estudio solo funciona con *IEXPLORER* y *FIREFOX*

Roboform2Go tiene problemas conocidos en el *AUTORUN* al insertarse en un sistema operativo diferente a *Windows*

Soporte principalmente en inglés

Riesgos inherentes asociados a un dispositivo extraíble (daño físico, corrupción de datos por virus, pérdida, etc)

Dashlane 4.1.1.10306

Es obligatorio una instalación local para poder utilizar la herramienta.

La aplicación web es de solo lectura.

No tiene log de accesos a la herramienta.

Las soluciones de doble factor de autenticación y OTP están orientadas al uso de una tercera herramienta cuyo proveedor es Yubico

La integración al navegador no es opcional

La extensión de Internet Explorer solo funciona con permisos de administrador.

Dashlane es partner de YUBICO por lo que publicitan la yubikey, la U2F es para cuantas Premium

Soporte principalmente en ingles

2.14 Otras características

Este aspecto contempla características adicionales por herramienta a la fecha de este análisis.

KeePass v.2.28

- Administración de contraseñas por grupos
- Se pueden colocar iconos para personalizar los grupos que se creen
- Hay campos adicionales para texto (detalles por cada contraseña)
- Se pueden configurar HOTKEYS
- Protección contra ataques de diccionario
- Bloqueo de área de trabajo: cuando se bloquea el equipo, se cambia de usuario, se suspende el equipo o demás, se pide nuevamente el *MASTER PASSWORD* para ingresar a la herramienta.
- No solo las contraseñas son cifradas sino también los nombres de usuarios, las notas, los comentarios, e incluso la fecha de creación, modificación, expiración y ultimo acceso a las entradas.

LastPass v.3.1.65

- Test de evaluación de las contraseñas de usuario a través de la funcionalidad "Desafío de Seguridad de *LastPass*". Indicara el progreso en cuanto al nivel de las contraseñas existentes, y se visualizaran las áreas en las cuales se puede mejorar la seguridad a través de alertas de seguridad.
- *LastPass* advierte de contraseñas débiles y duplicadas mientras se inicia sesión en la cuenta de usuario para poder generar nuevas de forma inmediata.

Roboform2Go v.7.9.9.1

- Tamaño reducido: aproximadamente 15MB
- Verificar consistencia de datos para asegurarse que están protegidos por el mismo *MASTER PASSWORD*.

Dashlane 4.1.1.10306

- Dashlane permite compartir datos (compartir información personal a través de email no es seguro) aunque en la versión gratuita, existe la limitación que solo se pueden compartir 5 elementos con cada persona.
- Funcionalidad de administración de dispositivos conocidos para acceder a los datos
- Funcionalidad de emergencia para dar acceso de solo lectura a contactos seleccionados (debe tener Dashlane instalado)
- Funcionalidad de Password Changer que sirve para, a partir de sitios conocidos, hacer la gestión de los cambios de contraseña de forma simplificada
- Ayuda para compras en línea (guarda recibos en la herramienta)
- Funcionalidad de Panel de seguridad que actúa como el desafío de seguridad de Lastpass para verificar la robustez de los datos almacenados.
- Verificación de identidad de navegadores

3. Incidentes Conocidos

Este ítem describe los principales incidentes que se han presentado con las herramientas analizadas en este estudio.

KeePass v.2.28

11/2014 [9] Una variante del troyano Citadel [10] se utiliza para infectar computadores y adquirir los *MASTER PASSWORD*s de *KeePass* y PasswordSafe. El sistema de doble factor de autenticación contribuye para contrarrestar este tipo de ataques.

LastPass v.3.1.65

05/2011[11] Se descubrió una anomalía en el tráfico de internet en la salida y entrada de datos. No se pudo determinar la causa del problema, sin

embargo dado el riesgo que teóricamente se hubieran copiado mails u otro dato de usuario como las contraseñas, *LastPass* decidió desmantelar los servidores involucrados y el 04/05/2011 solicitó a todos los usuarios cambiar sus *MASTER PASSWORD* por cuestiones de seguridad

08/2013 [12] Se reportó a una revista (la cual informo a *LastPass*) de un problema en el software el cual fue causado por una actualización reciente al sistema y permitía que al momento de realizar una descarga de la memoria o en el navegador, las contraseñas guardadas se pudieran leer en texto plano, no en asteriscos.

04/2014 [13] Cerca de 2 meses después del descubrimiento de *HEARTBLEED* [14], se descubrieron más vulnerabilidades de OpenSSL. Aunque las organizaciones deben actualizar sus servidores, los expertos en seguridad declaran que los fallos no son tan malos como *HEARTBLEED*.

CVE [15] identifica el fallo en TLS y las implementaciones DTLS en OpenSSL 1.0.1 donde no manejan correctamente los paquetes de extensión *HEARTBLEED*, lo que permite a atacantes remotos obtener información sensible de la memoria del proceso a través de paquetes ajustados que desencadenan un buffer de over-read, como se ha demostrado mediante la lectura de las claves privadas, relacionadas con d1_both.c y t1_lib.c, también conocido como el bug *HEARTBLEED*. Pese a que en CVE no se encuentra la publicación del sitio de la herramienta con el error mencionado, *LastPass* ha suministrado comunicados exponiendo la situación y las medidas que resolvió ejecutar cuando se presentaron los fallos.

La más crítica de las nuevas vulnerabilidades de OpenSSL se conoce como "Vulnerabilidad de inyección". En relación a *LastPass* hay que tener en cuenta que:

- Los datos almacenados en *LastPass* no se ven afectados por este error
- El *MASTER PASSWORD* nunca se comparte con *LastPass*
- El almacén de datos se cifra con AES de 256 bits antes de ser enviado a *LastPass* a través de SSL

- Las Bibliotecas SSL de los servidores han sido actualizadas con las últimas correcciones

Roboform2Go v.7.9.9.1

12/2010 *ROBOFORM* tuvo un problema relacionado a la licencia por el cambio de política de usuario. Esta política aplicaba a aquellos usuarios quienes desde 2004 habían adquirido *ROBOFORM* para sus PC, memoria *USB* u otros dispositivos. Ahora tendrían que pagar una anualidad con la que no se contaba antes. Con el cambio de política en las nuevas versiones, se suprimió la opción de poder exportar los datos de usuario con la *URL* completa haciendo compleja la exportación a otro tipo de gestor de contraseñas. El problema se solucionaba utilizando una versión anterior de *ROBOFORM* sin hacer la actualización a la última versión. Por supuesto lo anterior repercutió en descontento de los usuarios que eran fieles a *ROBOFORM*.

Dashlane 4.1.1.10306

Existen falsos positivos con algunos antivirus actualmente que identifican a Dashlane como un potencial virus. Esto también puede suceder debido a la manera en que funciona Dashlane ya que los datos se cifran de manera segura y se instalan extensiones en los navegadores para que se pueda completar la información directamente en la web, además que los datos se pueden sincronizar en los servidores y varios dispositivos. Lo anterior es considerado por algunos antivirus como sospechoso.

4. Calificación Gestores de Contraseñas evaluados

A continuación se califican los Gestores de Contraseñas analizados en este estudio, cada aspecto a evaluar tendrá un peso equivalente y una calificación de 0 a 3 donde 0 es el menor valor (denota ausencia del aspecto evaluado) y 3 el mejor (denota la opción más favorable entre las soluciones analizadas) considerando las características, ventajas y desventajas que

muestra cada solución. Los aspectos a evaluar fueron agrupados en las siguientes categorías:

- Confidencialidad
- Disponibilidad
- Integridad
- Resguardo de datos
- Privacidad
- Auditoria
- Facilidad de Uso

El resultado se explica en la última columna de la derecha describiendo el porqué de los valores asignados a cada Gestor de Contraseñas.

		KeePass 2 (Local)	*LastPass* (Online)	*Roboform2Go* (Portable)	Dashlane (Local/Online)	**Análisis de Calificación**
CONFIDENCIALIDAD	**Tipo de algoritmo para cifrar los datos**	3	3	2	3	*Roboform2Go* todavía ofrece la alternativa de utilizar Blowfish; dicha opción es menos favorable de acuerdo a que el algoritmo tiene ya muchos años en el mercado. Su problema reside en el tamaño de bloque el cual es de 64bits lo cual es considerado insuficiente para archivos de gran tamaño que son tan comunes en estos días. (Entre más grande sea el archivo y el tamaño del bloque sea pequeño, hay mayor probabilidad de un bloque repetido en el texto cifrado; estos bloques repetidos son bastante útiles en el criptoanálisis) [16] La opción más favorable es el AES.
	Ingreso a la herramienta	3	2	2	2	Todas las opciones funcionan con un *MASTER PASSWORD* para acceder a la BD, sin

						embargo *KeePass* al tener la alternativa de integrar un KEYFILE de entrada que se genera localmente, se constituye como la opción más favorable en este aspecto evaluado.
	Generador de contraseñas	3	3	3	3	Todas las soluciones generan contraseñas con un medidor de fortaleza de la contraseña.
	Protección del ingreso a la herramienta	3	3	0	3	*LastPass* utiliza PBKDF2 [17] para protección de ataques de fuerza bruta y de diccionario al *MASTER PASSWORD*. *KeePass* también implementa un mecanismo de protección contra ataques de diccionario. Dashlane también utiliza protección de número de ingresos.
	Protección de memoria RAM	3	0	3	0	*LastPass* en su versión estándar normal online no tiene incorporado el borrado de memoria. A diferencia de esto, *KeePass* borra el portapapeles cada vez que se hace la copia de la información. *Roboform2Go* por su parte borra la memoria cuando se desconecta la memoria *USB*. *Dashlane* a futuro piensa incorporar funcionalidades de protección de memoria, pero no es su foco.
	Seguridad en autocompletado	3	0	0	0	*KeePass* utiliza una doble técnica de envío de pulsaciones de teclas junto con la utilización del portapapeles, de forma que al realizar Escritura Automática, si el computador tiene algún software para capturar pulsaciones del teclado como un KEYLOGGER, es capaz de despistarlo. Esto es bastante útil en computadores de uso público no confiable.
	OTP	0	3	0	1	*LastPass* es la única opción que implementa sistema de OTP. Se genera un juego de claves las cuales pueden ser utilizadas solo una vez, una a una.

						Dashlane incorpora OTP pero es a partir de un tercero "Yubico OTP"
INTEGRIDAD	**Seguridad en BD**	3	3	3	3	La BD que almacena la contraseña en *KeePass* y *Roboform2Go* se cifra. En *LastPass y Dashlane* los datos se cifran localmente y luego se envían a la nube (se delega la confianza al fabricante).
DISPONIBILIDAD	**Servicio 7x24**	2	3	2	3	La opción online va a estar disponible siempre que se requiera y desde cualquier dispositivo (siempre y cuando haya conexión a internet y los servidores de *LastPass* estén funcionando correctamente) o sin conexión a internet instalando *LastPass* pocket o *LastPass* Portatil. En cualquier solución local se contara con el servicio 7x 24 siempre y cuando se cuente con la computadora con la aplicación instalada y la BD generada. Cualquier solución que sea instalable en una memoria *USB* estará sujeta a llevar consigo el dispositivo donde se tiene el software y la BD. *Dashlane* guarda localmente la información en la aplicación instalada y sincroniza contra servers de Dashlane
	Portabilidad de los datos	1	3	2	3	La solución de portabilidad es mejor en cuanto a un Gestor de Contraseñas online, debido a que independientemente del Sistema Operativo (*Windows*, *Linux* o Mac) y del navegador, se va a poder acceder a las contraseñas a través del sitio web, sin embargo dependerá de la confianza que tenga el usuario en la nube. En la solución local y la solución portable siempre se podrán llevar los datos a cualquier sitio si y solo si se cuenta con el dispositivo en el que fue instalado el software (Para una solución local se debe

						contar con el computador donde fue instalado el software y para la solución portable se debe contar siempre con el dispositivo extraíble donde se instaló)
RESGUARDO DE DATOS	**Backup de datos**	3	2	1	2	La mejor opción de exportación de BD es de *KeePass* debido a que tiene distintos formatos de salida y se puede integrar a otra herramienta, por ejemplo, pese a que el resguardo de datos no sea automático. *Dashlane* exporta legiblemente en xls o csv.
	Backup protegido	0	0	0	3	*Dashlane* exporta datos de manera segura para otro equipo que tena Dashlane instalado.
PRIVACIDAD	**Autocompletado**	3	3	3	3	Todas las opciones ofrecen autocompletado en los formularios, lo cual minimiza el riesgo de caer en un ataque de *PHISHING*
	Autenticación de doble factor	3	3	3	3	*LastPass* ofrece múltiples alternativas para la autenticación de doble factor. *Roboform2Go* ofrece dos opciones que son más complejas de utilizar y configurar. *KeePass* ofrece opciones de integración con cuentas de usuario y el KEYFILE *Dashlane* ofrece diversas soluciones pero deben ser integradas a través de una tercera herramienta.
AUDITORIA	**Trazabilidad**	3	3	0	1	*LastPass* y *KeePass* implementan medidas que permiten ver los registros de las entradas que el usuario ha ingresado a la herramienta. *Dashlane* únicamente guarda historial de contraseñas mostrando fecha de modificación.
FACILIDADES DE USO	**Sencillez de uso**	1	3	2	3	La opción que tiene más facilidad de uso es *LastPass*, su interfaz es la más intuitiva, adicionalmente la facilidad de uso a través de *LastPass*.com sin tener que instalarse lo hace la mejor opción.

	Idioma	2	2	2	2	Todos los ítems se califican de igual forma. Aunque para todas las opciones involucradas los manuales, las páginas y el soporte no se encuentra completamente documentado en español.
	Plataforma	2	3	1	2	*KeePass* y *LastPass* son multiplataforma aunque debido a la facilidad de acceder desde cualquier dispositivo, *LastPass* se lleva la ventaja. *Roboform2Go* tiene la limitación de ser solo *Windows* principalmente y solo integrarse con *IEXPLORER* y *FIREFOX* *Dashlane* no funciona en Linux
	Integración con navegadores	1	3	2	2	*LastPass* es la solución más común de integrar con otros navegadores. *KeePass* es la peor calificada de acuerdo a la complejidad que exige la instalación del *PLUGIN* para la integración con el navegador. *Roboform2Go* solo puede integrarse con *IEXPLORER* y *FIREFOX* *Dashlane* tiene problemas para funcionar adecuadamente en Internet Explorer
	Medidor de calidad de contraseñas	3	3	3	3	Todas las opciones incluyen un medidor de contraseñas seguras.

Tabla 3: Calificación Gestores de Contraseñas

5. Resultados Comparativa

A partir de las calificaciones obtenidas en la tabla anterior, se generan los valores de los grupos definidos agrupándolos en ponderadores, cada ponderador es el promedio de los aspectos evaluados por cada grupo, al final la suma de todos los grupos por cada Gestor de Contraseñas determina la calificación final de las soluciones descritas en este estudio.

	Kepass2 Ver. 2.28	*LastPass* Ver. 3.1.65	*Roboform2Go* Ver. 7.9.9.1	*Dashlane* Ver. *4.1.1.10306*
Ponderador Confidencialidad	2,57	2,00	1,43	1,71
Ponderador Integridad	3	3	3	3
Ponderador Disponibilidad	1,5	3	2	3
Ponderador Resguardo de Datos	1,5	1	0,5	2,5
Ponderador Privacidad	3	3	3	3
Ponderador Auditoria	3	3	0	1
Ponderador Facilidad	1,8	2,8	2	2,4
TOTAL	**16,37**	**17,80**	**11,93**	**16,61**

Tabla 4: Resultados Calificación

La herramienta *LastPass* es la que obtuvo el mejor puntaje de acuerdo a que sobresale en aspectos como la disponibilidad y la facilidad de uso ya que es bastante intuitiva y posee niveles adecuados de seguridad pese a que tiene aspectos por mejorar como el idioma de soporte y la seguridad en el autocompletado.

Por otra parte, la herramienta *Roboform2Go* es la que obtuvo el menor puntaje ya que carece de aspectos importantes como la protección contra ataques de fuerza bruta, no tiene seguridad en el autocompletado y le hace falta el componente que permite ver la trazabilidad del usuario.

La herramienta *KeePass* pese a ser la solución más técnica, carece de facilidad de uso, debido a que si bien para un **usuario avanzado** al ser altamente configurable puede ser la mejor herramienta, para un **usuario común** puede suponer dificultad su uso en aspectos por ejemplo como la sincronización.

IV. Recomendaciones

1. Recomendaciones a usuarios personales

La recomendación para los usuarios que son menos expertos y que no hace falta que utilicen un gestor de contraseñas debido a que manejan por ejemplo solo dos servicios (y tengan buena memoria), es utilizar contraseñas fuertes con letras (mayúsculas y minúsculas), números, y caracteres especiales (Ver Buenas Practicas de Seguridad descritas en este documento). El PASSPHRASE también puede ser una alternativa útil para este tipo de usuarios ya que representa una solución que no incurre en gastos ni herramientas adicionales.

La recomendación para usuarios que utilizan varias contraseñas es utilizar una solución de Gestor de Contraseñas que se ajuste a sus necesidades. Si bien los gestores de contraseñas facilitan la administración de las contraseñas de un usuario, cada sistema por su parte tiene sus pros y contras. En este sentido se hacen las siguientes recomendaciones para elegir un Gestor de Contraseñas:

- Asegurar cuentas de usuario del sistema operativo: El *MASTER PASSWORD* es la primera línea de defensa en un Gestor de Contraseñas, sin embargo, es buena práctica asegurarse de que la cuenta de usuario del sistema operativo donde está instalada la aplicación también este bien protegida al menos con una contraseña lo suficientemente robusta.

- Lo mejor para el usuario: El usuario debe asegurarse que su solución se ajuste a sus necesidades en términos de costos, seguridad y facilidad de uso.

- Únicamente utilizar las soluciones reconocidas y de confianza: Tener especial cuidado con las soluciones que tienen mucho tiempo en el mercado y no tienen ninguna retroalimentación que avale su confianza

(distintas a las presentadas por este estudio). Pueden ofrecerse soluciones disfrazadas desarrolladas para únicamente robar los datos de usuario así que es necesario asegurarse de que todas las soluciones que se elijan sean actualizadas constantemente y se esté usando la versión más reciente.

- La solución debe ser simple de usar: debido a que si se encuentra una solución demasiado compleja, se pueden cometer errores que dejen expuesto al usuario.

- Toda solución de Gestor de Contraseñas debe utilizar un estándar de cifrado fuerte reconocido internacionalmente: Hay que tener especial atención con algunas soluciones que son patrocinadas o son de propietarios desconocidos que utilizan sus propios algoritmos criptográficos.

- El gestor de contraseñas que se elija debería poder ejecutarse en los diferentes equipos que utilice el usuario (para facilidad de este). Algunas soluciones incluyen versiones que funcionan en dispositivos móviles.

- Sincronización de datos: La opción de sincronización es un plus importante al momento de elegir la solución, sin embargo, es menester asegurarse que la herramienta cifre los datos localmente antes de enviarlos al sistema central para evitar el riesgo de un posible ataque a la red que intercepte los datos por ejemplo.

- Seguridad en la generación de Contraseñas: La solución debe tener la opción de generar contraseñas aleatorias y alertar para el control de la caducidad de las contraseñas, adicionalmente toda solución debería tener un medidor de la calidad de las contraseñas para generar contraseñas seguras facilitando al usuario el tener que crear las contraseñas sin saber si es segura o no.

- Tener cuidado al ingresar el *MASTER PASSWORD*: si el usuario elige una solución que está integrada al Navegador, es necesario asegurarse que no se guarde automáticamente el *MASTER PASSWORD* en el Navegador. Si se guarda y no se tiene un doble factor de autenticación activo, los datos quedaran expuestos a cualquier usuario que ingrese con el navegador o si se ataca el sistema de gestión de contraseñas del navegador, se podrán obtener los datos.

2. Recomendaciones a Organizaciones

En general las organizaciones cuentan con infraestructura propia para utilizar una solución que sea robusta y adecuada a sus necesidades. En muchos casos, las organizaciones utilizan sistemas de SSO donde al utilizar la clave de autenticación al dominio, el usuario va a estar en la facultad de poder acceder a la mayoría de los sitios y herramientas que proporciona la organización sin la necesidad de usar diversas contraseñas. No obstante lo anterior, al diversificarse los accesos a sistemas específicos nuevos que requieran autenticación, el anexar servicios y accesos al sistema de SSO supone una complejidad que puede ser minimizada si se utiliza una herramienta para gestionar las contraseñas específicas para sistemas por fuera del SSO.

En este sentido la solución de Sistema Gestor de Contraseñas que use la organización deberá mínimamente:

- ser instalada de manera local en los servidores de la organización
- ser sincronizado frecuentemente
- incluir auditoria para poder hacer trazabilidad de su uso
- poseer un nivel de configuración de seguridad adecuado para generar y utilizar las contraseñas
- de ser un sistema de software libre, restringir la instalación de complementos y demás que comprometan la seguridad de los datos del usuario

- cumplir con los requerimientos legales tanto de la organización como de entes externos si aplica.

Según este estudio, la solución más favorable para una organización sería la de *KeePass*, el factor de complejidad de la configuración de la herramienta estará a cargo de la organización con personal calificado para realizar la parametrización correspondiente.

V. Conclusiones

La principal conclusión del estudio realizado en este documento es que para cualquier usuario (común o avanzado), es necesario utilizar un sistema de gestión de contraseñas si se utilizan varias cuentas de usuario. Si la herramienta es usada conociendo las mínimas prestaciones, lo anterior principalmente redundará en tener contraseñas robustas y distintas para cada cuenta de usuario.

Si la solución de Sistema Gestor de Contraseñas que se implementa tiene doble factor de autenticación, será una opción más que adecuada debido a que independiente que el *MASTER PASSWORD* sea sencillo o complejo, no se podrá acceder a los datos si no se tiene el otro factor de autenticación. Adicionalmente, la herramienta debería tener protección controlando el número de intentos de ingreso de contraseña fallidos a una cuenta así como el control de número de intentos a nombres de usuario con una misma contraseña para evitar ataques de fuerza bruta o diccionario.

Uno de los aspectos que más le quita puntos a *LastPass* es que la herramienta esté disponible en español, pero que en realidad cuando se navega a través de esta hay secciones enteras en inglés. Independiente de lo anterior, la ayuda de *LastPass* es más amigable y se encuentra dentro de la misma página desde donde accede la herramienta.

La opción de sincronización del archivo de BD de *KeePass* de manera online carece de practicidad a la hora de lograr tener actualizados los datos y la solución que ofrece complicaría a un usuario sin conocimientos técnicos o que no posea acceso a un servidor ftp por ejemplo.

Las características adicionales de la herramienta *Dashlane* para compartir contraseñas y el uso de emergencia la hacen una opción interesante para cualquier tipo de usuario, sin embargo aspectos como la configuración del doble factor de autenticación, que esté ligado a un tercero

y que por ejemplo las Yubikey solo funcionen con la cuenta Premium (con coste adicional) complejizan la determinación a la hora de elegirla como solución.

En relación a la calificación para los gestores de contraseñas analizados se resalta que:

- La solución de *Roboform2Go* debería implementar un sistema que proteja de ataques de diccionario o fuerza bruta debido a que se pueden realizar muchos intentos fallidos de ingreso sin que se bloquee la cuenta por un tiempo determinado por ejemplo.
- Para las soluciones de *Roboform2Go, Dashlane y LastPass* el generar un mecanismo de autocompletado seguro que pueda engañar o despistar a un posible atacante que tenga instalado por ejemplo un KEYLOGGER en el computador añade un nivel de seguridad adicional.
- *KeePass*, *LastPass* y *Roboform2Go* deberían proteger la copia de respaldo que se genera al exportar los datos al menos con el *MASTER PASSWORD*. En el caso de *Dashlane* este aspecto es el punto más significativo a favor ya que permite la exportación de archivo seguro en formato .DASH.
- *Roboform2Go* debería generar un log de seguridad que permita realizar la trazabilidad de las acciones que se han realizado por parte el usuario a la herramienta.
- *Dashlane* debería incorporar log de accesos.

La solución de *KeePass* es la más técnica y la más segura por todos los aspectos de parametrización que contiene, sin embargo es la opción menos conveniente por el grado de complejidad que implica la configuración de estos. La solución online *LastPass* es la más conveniente debido a su facilidad de uso, doble factor de autenticación y aspectos de seguridad para evitar el robo local de datos, sin embargo, al elegir esta opción no se tiene el control sobre en donde esta guardada la información.

VI. Glosario

Autenticación: [18] la autenticación es el proceso de intento de verificar la identidad digital del remitente de una comunicación como una petición para conectarse. El remitente siendo autenticado puede ser una persona que usa un ordenador, un ordenador por sí mismo o un programa del ordenador. En un web de confianza, "autenticación" es un modo de asegurar que los usuarios son quién ellos dicen que ellos son - que el usuario que intenta realizar funciones en un sistema es de hecho el usuario que tiene la autorización para hacer así.

Confidencialidad: [19] es la propiedad de la información, por la que se garantiza que es accesible únicamente por el personal autorizado a acceder a dicha información. En este contexto, evaluar por cada herramienta: criptografía de datos, tipo de algoritmo, generador de contraseñas, caducidad de contraseña.

Contraseña: acreditación de identidad que permitirá acceder a la información precisa que se necesite en el momento determinado.

Disponibilidad: [19] es la propiedad de la información por la que se garantiza que la información está dispuesta cada vez que se requiera. En este contexto, evaluar por cada herramienta: servicio 7x24 y que se pueda usar en cualquier sitio (portabilidad)

Facilidades de uso: son las características adicionales que poseen las herramientas y que facilitan el uso de la herramienta para un usuario. En este contexto, evaluar por cada herramienta.

GPL (General Public Licence): [20] tipo de licencia que garantiza a los usuarios finales (personas, organizaciones, compañías) la libertad de usar, estudiar, compartir (copiar) y modificar el software.

HOTKEY: [21] combinación de teclas que si se presionan simultáneamente, realizan acciones durante el uso de un software.

Integridad: [19] es la propiedad de la información por la que se garantiza que no se altera o modifica la información. En este contexto, evaluar por cada herramienta que la BD de contraseñas no pueda ser alterada o modificada.

KEYLOGGER: [22] software o hardware específico que captura las pulsaciones del teclado almacenándolas en un archivo.

Malware: [23] software que tiene como objetivo infiltrarse y o dañar un Sistema de información

Máquina virtual: [24] una máquina virtual es un contenedor de software perfectamente aislado que puede ejecutar sus propios sistemas operativos y aplicaciones como si fuera un ordenador físico. Una máquina virtual se comporta exactamente igual que lo hace un ordenador físico y contiene sus propios CPU, RAM, disco duro y tarjetas de interfaz de red (NIC) virtuales.

***MASTER PASSWORD*:** contraseña Maestra que se utiliza para asegurar el ingreso a un software determinado.

Passphrase (Frase de Contraseña): [25] una frase de contraseña es una cadena de palabras o caracteres que sirve para controlar el acceso a una red o un programa.

PBKDF2 (Password-Based Key Derivation Function 2) [17]: Contraseña de fortalecimiento de algoritmo para prevenir éxito en ataque de fuerza bruta.

Resguardo de datos: [26] es la copia de los datos de usuario originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de pérdida de los datos en la herramienta. En este contexto, evaluar por cada herramienta: posibilidad de realizar backup de los datos de usuario y si está protegido el backup.

VII. Anexos

Anexo I: ENCUESTA SOBRE USO Y CONOCIMIENTO DE GESTORES DE CONTRASEÑAS

Estructura de la Encuesta sobre uso de gestores de contraseñas

A continuación se presenta la estructura de la encuesta que se realizó:

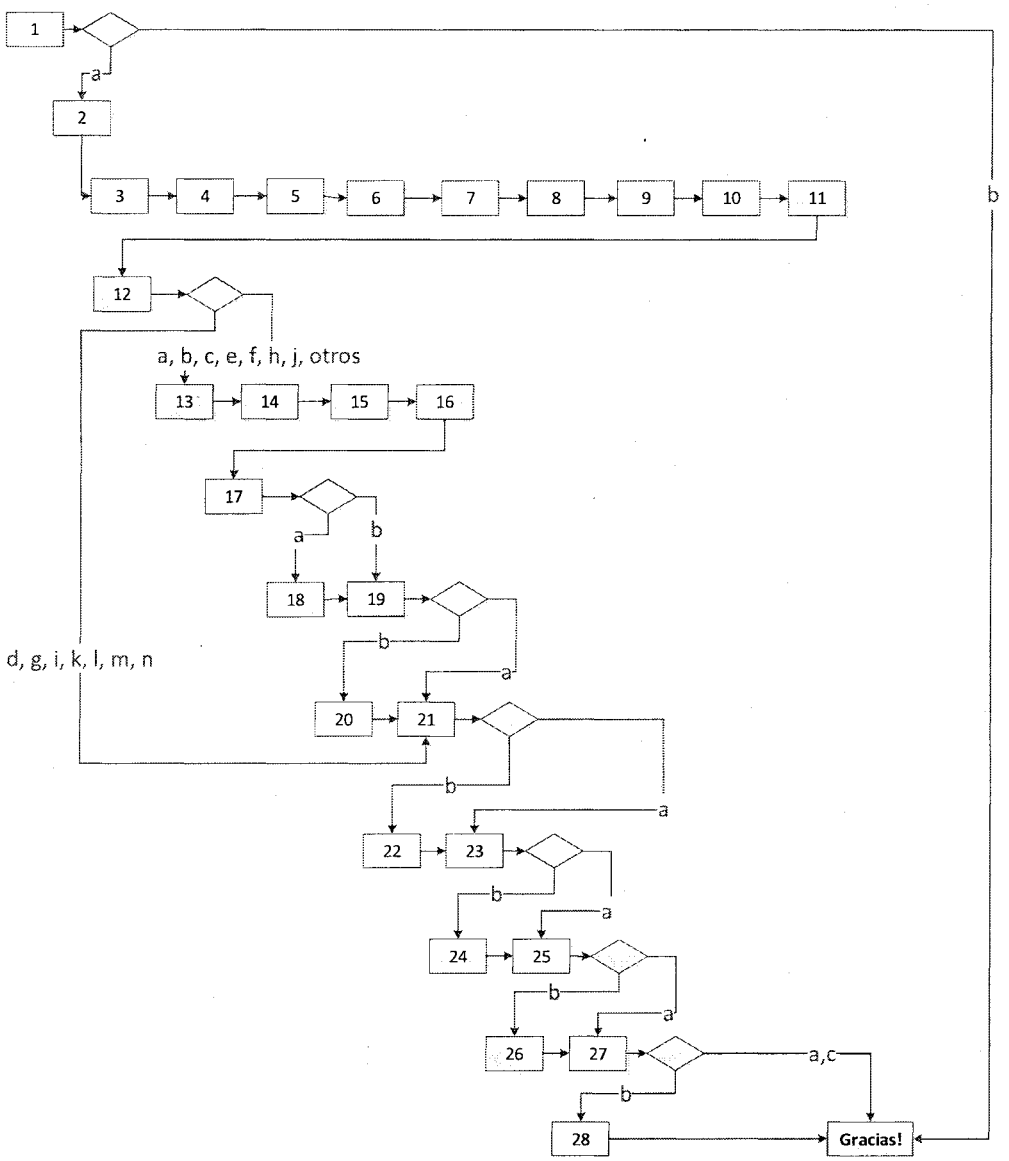


Ilustración 6 Encuesta sobre uso de Gestores de Contraseñas

Resultados de la Encuesta

En total, se realizó satisfactoriamente la encuesta a 184 personas de manera aleatoria que residen en diferentes países a nivel global (Argentina, Brasil, Canadá, Colombia, Costa Rica, Ecuador, Holanda, Honduras, República Dominicana, Uruguay). La encuesta se desarrolló durante el segundo semestre de 2013 y se publicó el mes de marzo de 2014 teniendo una vigencia de 2 meses. El siguiente grafico detalla la cantidad de respuestas por día durante la vigencia de la publicación:

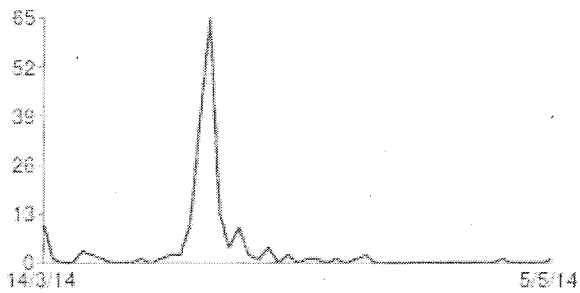


Ilustración 7 Numero de respuestas diarias

Las respuestas de las preguntas que no fueron señaladas por ninguno de los encuestados se desestimaron del enunciado de resultados de la encuesta.

A continuación se exponen los resultados de la encuesta:

Datos de Participante

En este apartado se recopila información general acerca del participante.

- Es hombre o mujer:

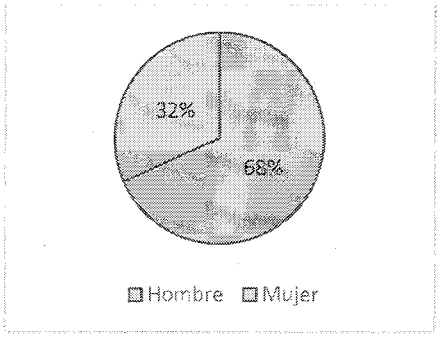


Ilustración 8 Genero del encuestado

Hombre	68%
Mujer	32%

- Elija el rango de edades en el que usted se encuentra:

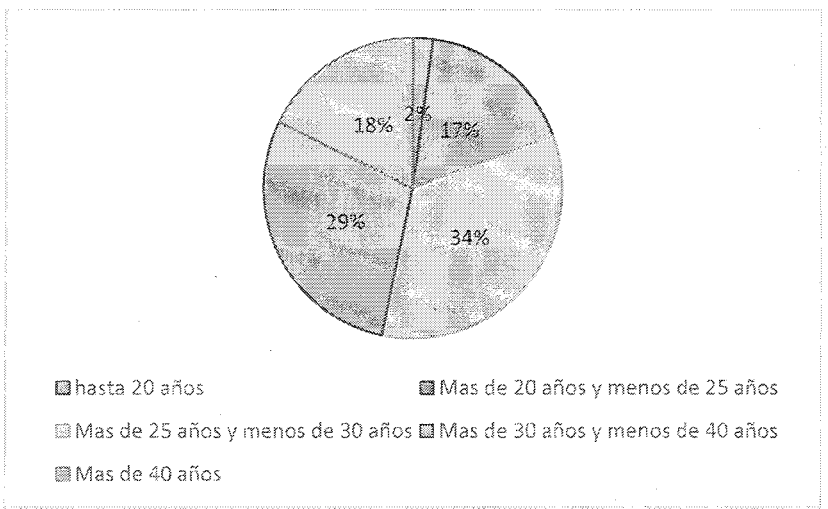


Ilustración 9 Edad del Encuestado

hasta 20 años	2%
Más de 20 años y menos de 25 años	18%
Más de 25 años y menos de 30 años	33%
Más de 30 años y menos de 40 años	29%

Más de 40 años	18%

- Indique el grado máximo de formación académica que posee:

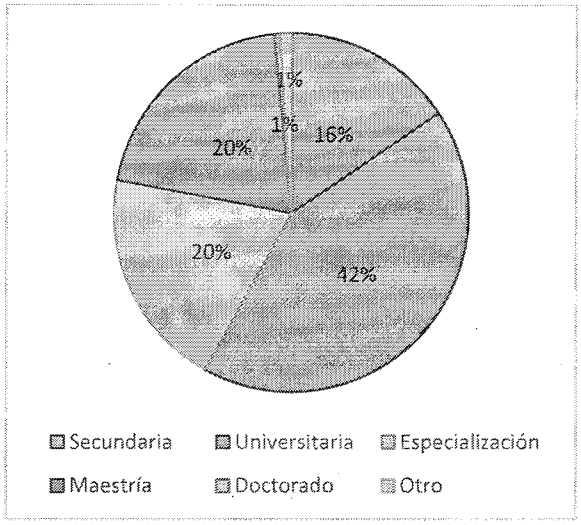


Ilustración 10 Formación académica del encuestado

Secundaria	16%
Universitaria	42%
Especialización	20%
Maestría	20%
Doctorado	1%
Otro	1%

- Indique su país de residencia actualmente:

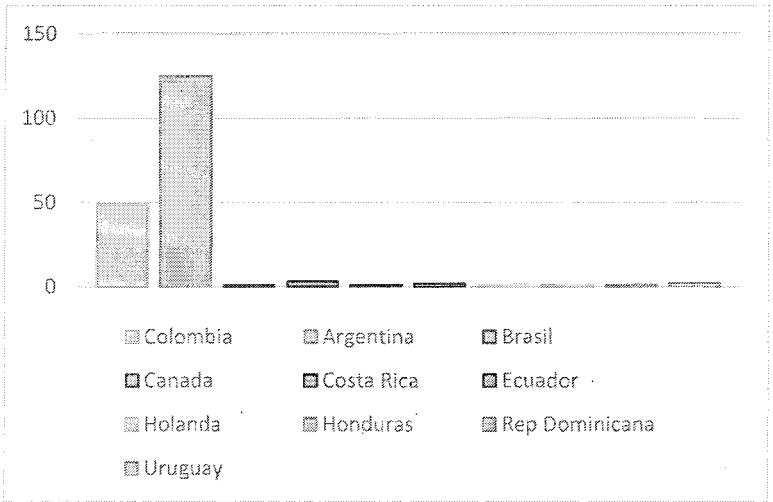


Ilustración 11 País de residencia del encuestado

Colombia	26,3%
Argentina	67,2%
Brasil	0,5%
Canada	1,6%
Costa Rica	0,5%
Ecuador	1,1%
Holanda	0,5%
Honduras	0,5%
Rep Dominicana	0,5%
Uruguay	1,1%

- Indique el área en que se desempeña laboralmente:

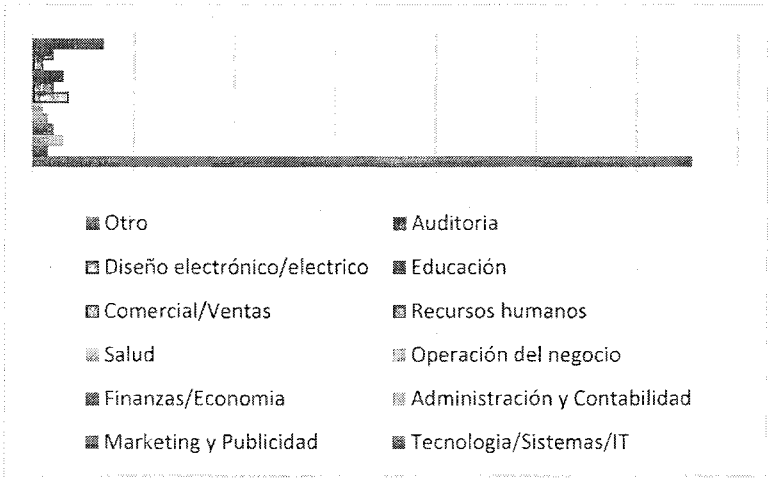


Ilustración 12 Sector laboral del encuestado

Tecnología/Sistemas/IT	70,4%
Marketing y Publicidad	1,6%
Administración y Contabilidad	3,2%
Finanzas/Economía	2,2%
Operación del negocio	1,6%
Salud	1,1%
Recursos humanos	3,8%
Comercial/Ventas	2,2%
Educación	3,2%
Diseño electrónico/eléctrico	1,1%
Auditoria	2,2%
Otro	7,5%

- Indique la jerarquía del puesto en el que se desempeña:

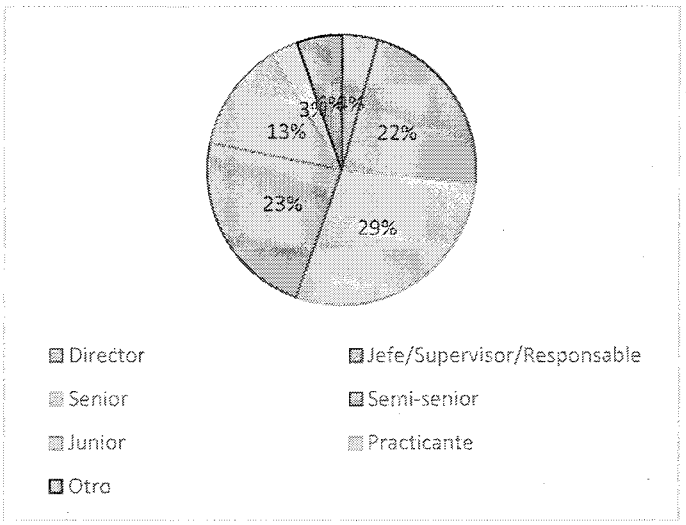


Ilustración 13 Jerarquía del encuestado

Director	4%
Jefe/Supervisor/Responsable	22%
Senior	29%
Semi-senior	23%
Junior	13%
Practicante	3%
Otro	6%

Generalidades

1. ¿Utiliza más de un servicio que requiera inicio de sesión a través de Internet?

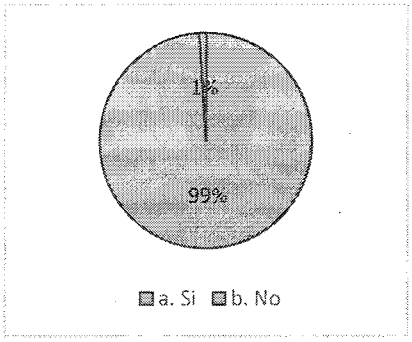


Ilustración 14 Uso de servicios a través de Internet

a. Si 99%

b. No 1%

A partir de la pregunta anterior se define que se van a trabajar con 182 encuestas.

2. ¿Qué servicios?

a. Gmail	**163**	90%
b. Yahoo	**61**	34%
c. Outlook	**130**	71%
d. Homebanking	**120**	66%
e. Youtube	**108**	59%
f. Skype	**144**	79%
g. Facebook	**154**	85%
h. Twitter	**98**	54%
i. Zonajobs	**63**	35%
Otro	**20**	11%

3. En su opinión, ¿las contraseñas que utiliza para acceder a esos servicios son confiables?

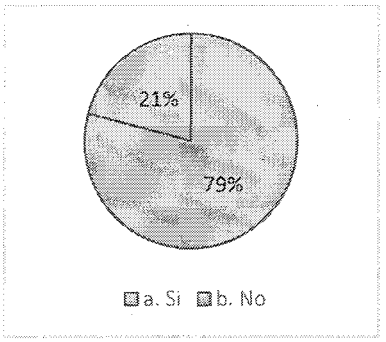


Ilustración 15 Confianza en las contraseñas propias

a. Si 79%

b. No 21%

4. ¿Las contraseñas que utiliza tienen una longitud mayor a 8 caracteres?

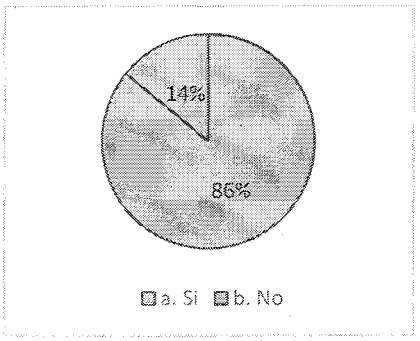


Ilustración 16 Longitud de contraseña

a. Si 86%

b. No 14%

5. ¿Las contraseñas que utiliza son de fácil asociación a documentos, información dependiente de usted o email?

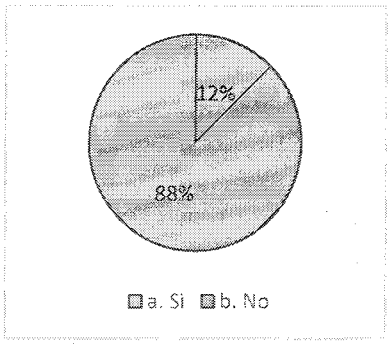


Ilustración 17 Asociación de contraseñas a datos del usuario

a. Si 12%

b. No 88%

6. ¿Utiliza combinaciones de letras con números y caracteres especiales para crear sus contraseñas?

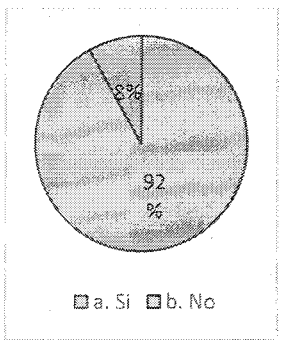


Ilustración 18 Caracteres y letras con números en contraseñas

a. Si 92%

b. No 8%

7. Cuando cambia de contraseña, ¿esta difiere de la anterior notoriamente?

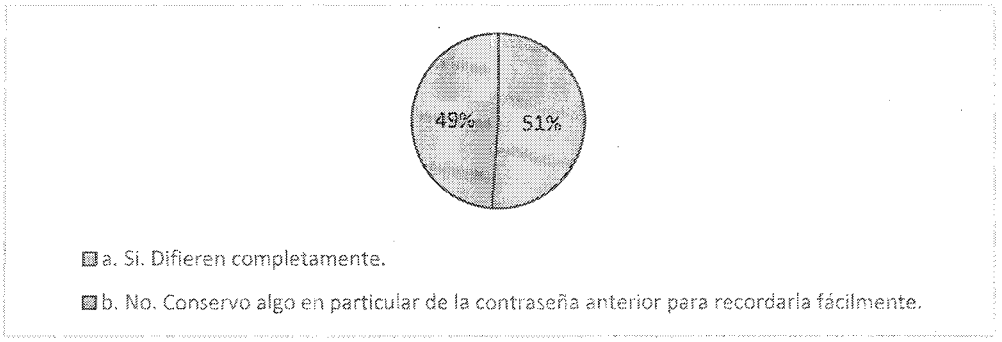


Ilustración 19 Cambio de contraseña

a. Si. Difieren completamente.	51%
b. No. Conservo algo en particular de la contraseña anterior para recordarla fácilmente.	49%

8. ¿Alguna vez ha olvidado una contraseña?

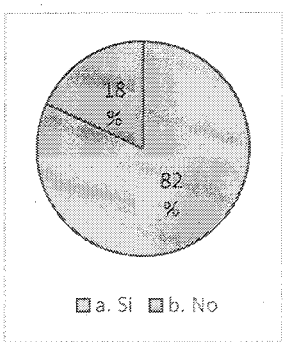


Ilustración 20 Olvido de contraseña

a. Si	82%
b. No	18%

9. ¿Utiliza la misma contraseña o alguna similar para más de un servicio?

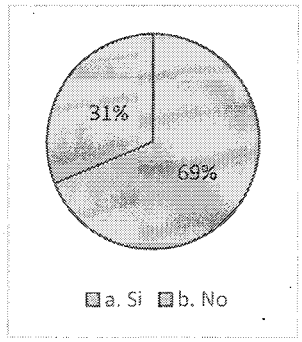


Ilustración 21 Uso de contraseña para más de un servicio

a. Si 69%

b. No 31%

10. ¿Cada cuánto cambia sus contraseñas?

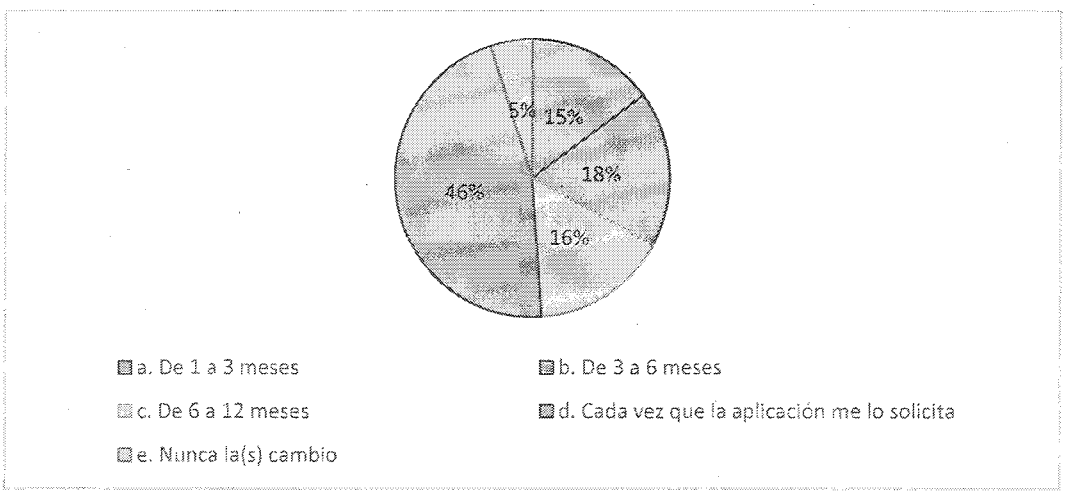


Ilustración 22 Periodicidad de cambio de la contraseña

a. De 1 a 3 meses 15%

b. De 3 a 6 meses 18%

c. De 6 a 12 meses 16%

d. Cada vez que la aplicación me lo solicita 46%

e. Nunca la(s) cambio 5%

11. ¿Usa una frase de contraseña (PASSPHRASE) para definir la contraseña?

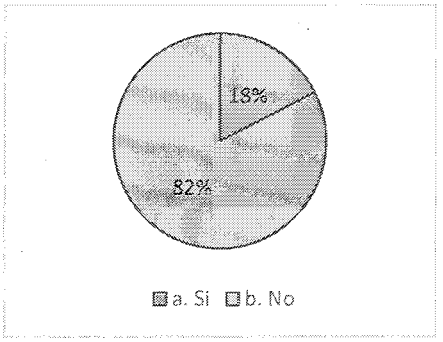


Ilustración 23 Uso de PASSPHRASE para contraseña

a. Si 18%

b. No 82%

12. ¿Cómo administra sus contraseñas?

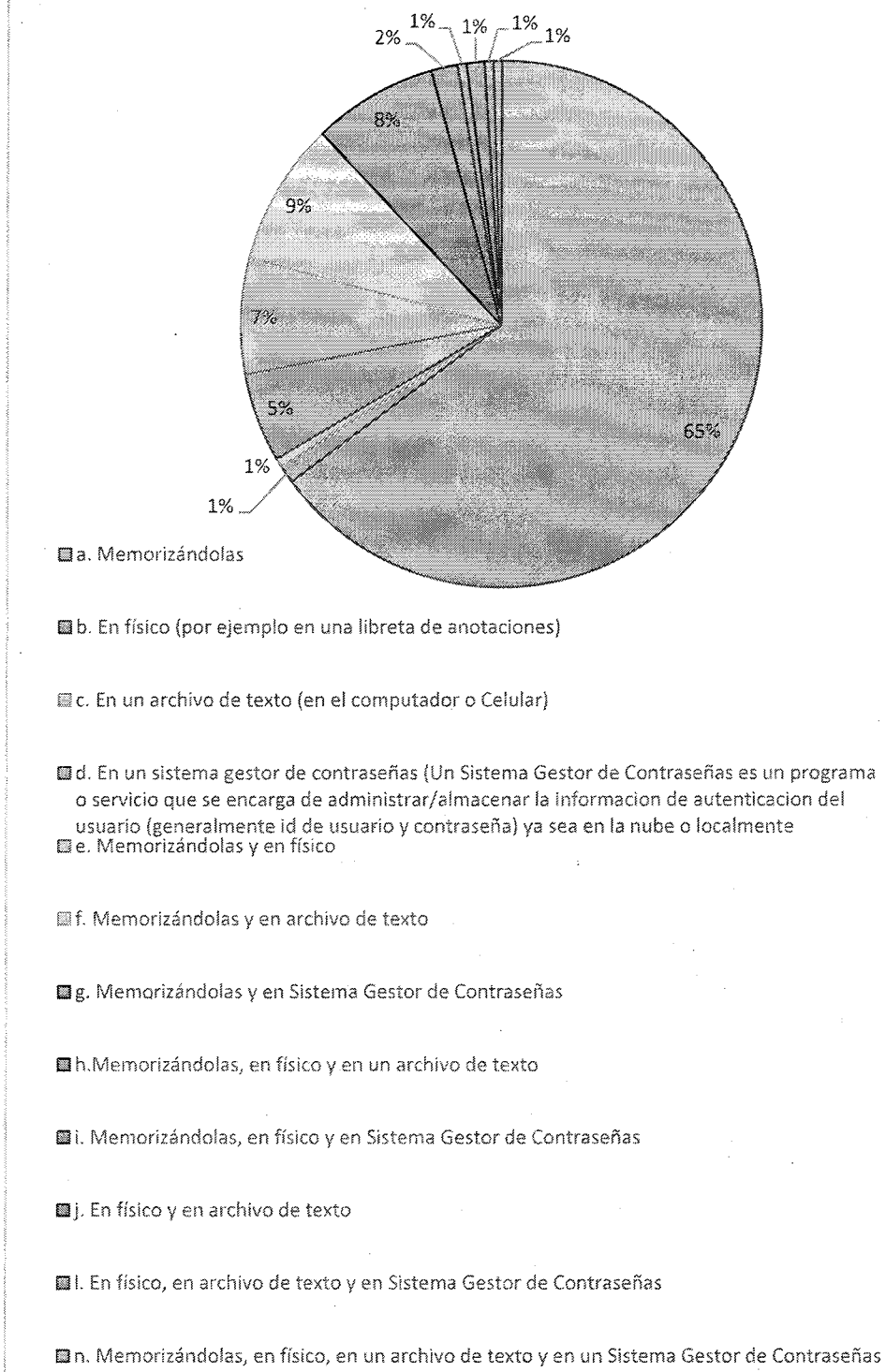


Ilustración 24 Administración de contraseñas

a. Memorizándolas	65%
b. En físico (por ejemplo en una libreta de anotaciones)	1%
c. En un archivo de texto (en el computador o Celular)	1%
d. En un sistema gestor de contraseñas (Un Sistema Gestor de Contraseñas es un software o servicio que se encarga de administrar/almacenar la información de autenticación del usuario (generalmente id de usuario y contraseña) ya sea en la nube o localmente)	5%
e. Memorizándolas y en físico	7%
f. Memorizándolas y en archivo de texto	9%
g. Memorizándolas y en Sistema Gestor de Contraseñas	8%
h. Memorizándolas, en físico y en un archivo de texto	2%
i. Memorizándolas, en físico y en Sistema Gestor de Contraseñas	1%
j. En físico y en archivo de texto	1%
l. En físico, en archivo de texto y en Sistema Gestor de Contraseñas	1%
n. Memorizándolas, en físico, en un archivo de texto y en un Sistema Gestor de Contraseñas	1%

A partir de lo anterior se visualiza que únicamente un 15% de las personas encuestadas utilizan algún sistema de gestión de contraseñas para administrar sus cuentas de usuario. Las preguntas posteriores están sujetas a ese conjunto de datos.

13. ¿Qué Gestor de Contraseñas utiliza?

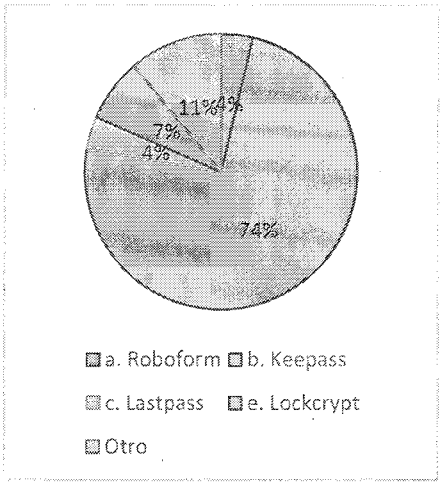


Ilustración 25 Gestores de contraseñas utilizados

a. *ROBOFORM*	4%
b. *KeePass*	74%
c. *LastPass*	4%
e. Lockcrypt	7%
Otro	11%

14. ¿Porque utiliza este Gestor de Contraseñas?

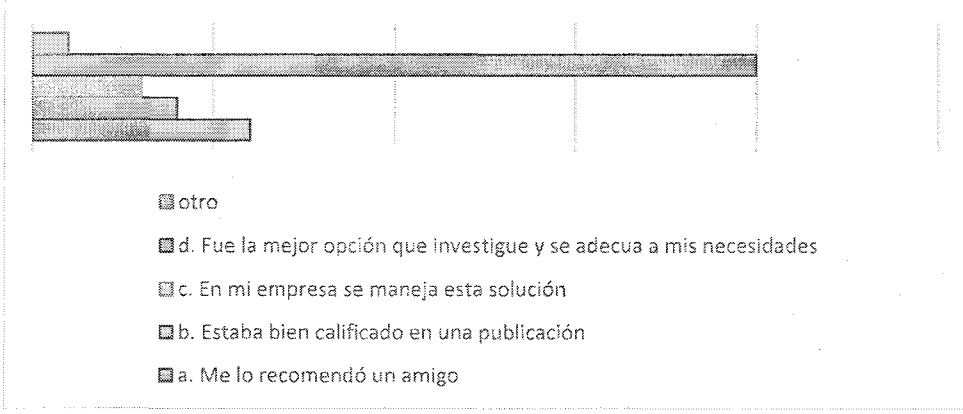


Ilustración 26 Razón de uso del Gestor de Contraseñas

a. Me lo recomendó un amigo	21%
b. Estaba bien calificado en una publicación	14%
c. En mi empresa se maneja esta solución	7%
d. Fue la mejor opción que investigue y se adecua a mis necesidades	55%
Otro	3%

15. ¿Qué características conoce brinda el Gestor de Contraseñas que utiliza actualmente?

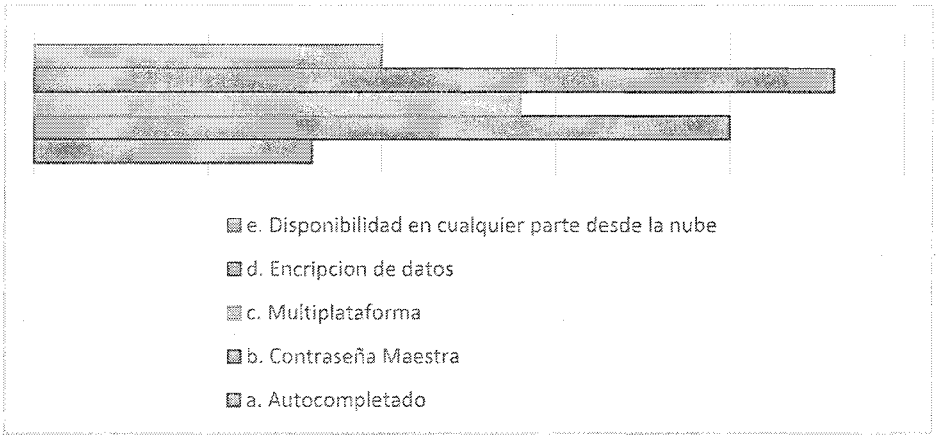


Ilustración 27 Características del gestor de contraseñas

a. Autocompletado	**8**	10,7%
b. *MASTER PASSWORD*	**20**	26,7%
c. Multiplataforma	**14**	18,7%
d. Criptografía de datos	**23**	30,7%
e. Disponibilidad en cualquier parte desde la nube	**11**	13,3%

16. ¿Porque lo considera apropiado para sus necesidades?

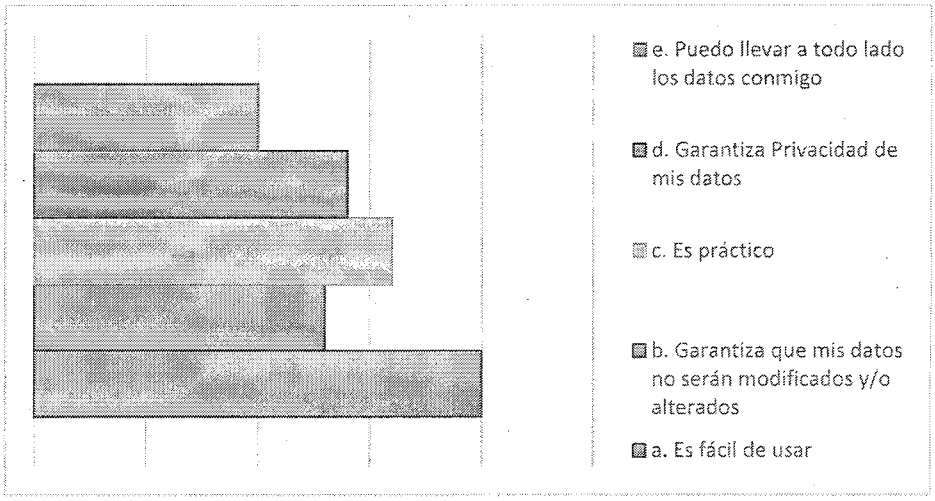


Ilustración 28 Motivación de elección del gestor de contraseñas

a. Es fácil de usar	74%
b. Garantiza que mis datos no serán modificados y/o alterados	48%
c. Es práctico	59%
d. Garantiza Privacidad de mis datos	51%
e. Puedo llevar a todo lado los datos conmigo	37%

17. ¿En caso de pérdida o daño de su PC/Celular (donde se estén guardando los datos), o falta de acceso al servicio que tenga en la nube, tiene una copia de respaldo de la información?

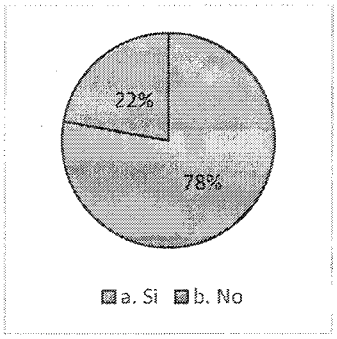


Ilustración 29 Copia de respaldo de datos de usuario

a. Si 79%

b. No 21%

Positivo 17.

18. ¿Cómo conserva su copia de respaldo?

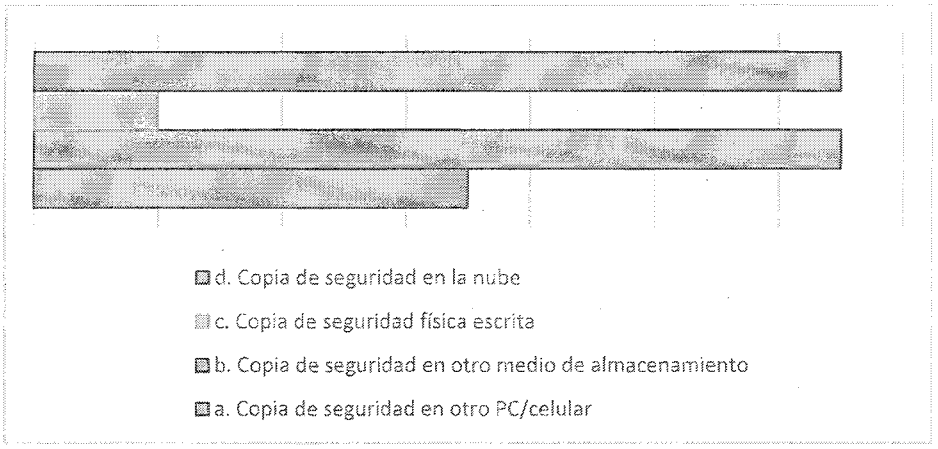


Ilustración 30 Forma de guardar copia de respaldo

a. Copia de seguridad en otro PC/celular 33%

b. Copia de seguridad en otro medio de almacenamiento 62%

c. Copia de seguridad física escrita 9%

d. Copia de seguridad en la nube 62%

Satisfacción con la elección

19. ¿Está satisfecho con la elección de su Gestor de Contraseñas?

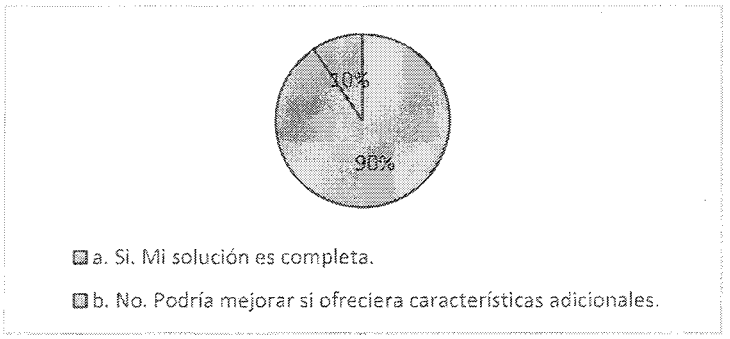


Ilustración 31 Satisfacción de uso

a. Si. Mi solución es completa. 90%

b. No. Podría mejorar si ofreciera características adicionales. 10%

Negativo 19.

20. ¿Qué característica(s) adicional(es) le hace(n) falta a su Gestor de Contraseñas?

c. Acceso desde cualquier parte 67%

e. Exportación de datos 33%

Tipos de Sistemas Gestores de Contraseñas

Gestor de Contraseñas Local

En relación al conocimiento de los diferentes tipos de gestores de contraseñas se toman en consideración las 182 encuestas.

21. ¿Considera seguro delegar id de usuario y contraseña a un Gestor de Contraseñas local?

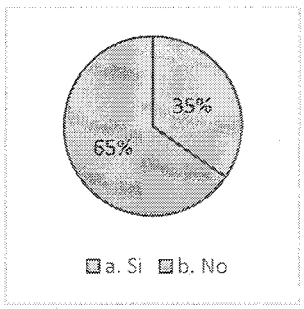


Ilustración 32 Confianza en Gestor de Contraseñas local

a. Si 35%

b. No 65%

Negativo 21.

22. En caso negativo ¿porque?

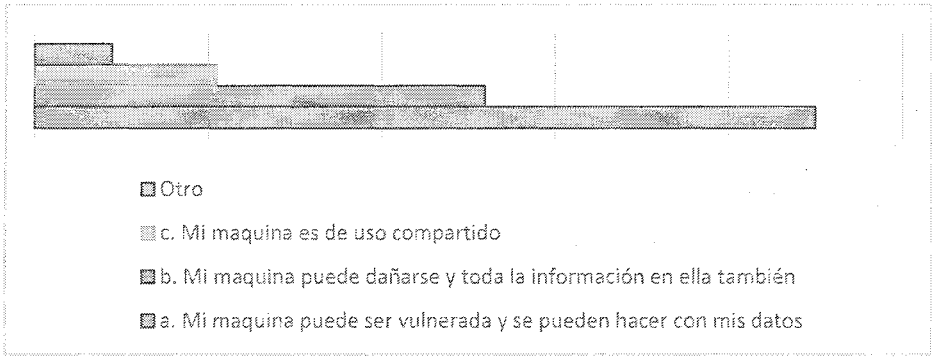


Ilustración 33 Desconfianza en gestor de contraseñas local

a. Mi maquina puede ser vulnerada y se pueden hacer con mis datos	78%
b. Mi maquina puede dañarse y toda la información en ella también	45%
c. Mi maquina es de uso compartido	18%
Otro	8%

Gestor de Contraseñas Online

23. ¿Considera seguro delegar id de usuario y contraseña a un Gestor de Contraseñas online?

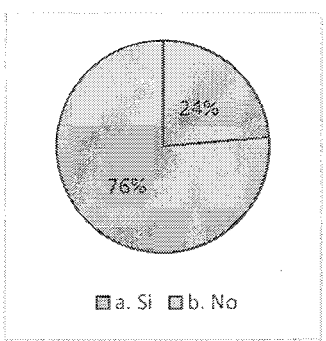


Ilustración 34 Confianza en gestor de contraseñas online

a. Si 23%

b. No 77%

Negativo 23.

24. En caso Negativo, ¿porque?

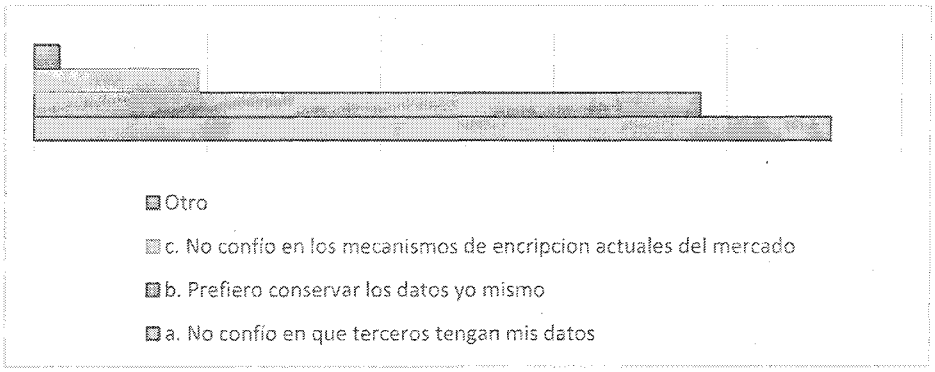


Ilustración 35 Desconfianza en gestor de contraseñas online

a. No confío en que terceros tengan mis datos	66%
b. Prefiero conservar los datos yo mismo	55%
c. No confío en los mecanismos de Criptografía actuales del mercado	14%
Otro	2%

Gestor de Contraseñas Portable

25. ¿Considera seguro delegar id de usuario y contraseña a un Gestor de Contraseñas Portable?

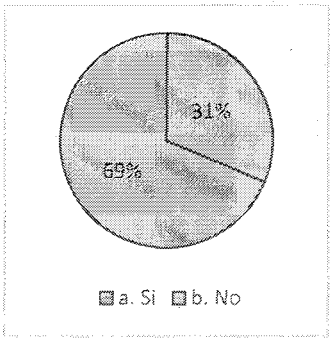


Ilustración 36 Confianza en gestor de contraseñas portable

a. Si 31%

b. No 69%

Negativo 25.

26. En caso negativo, ¿porque?

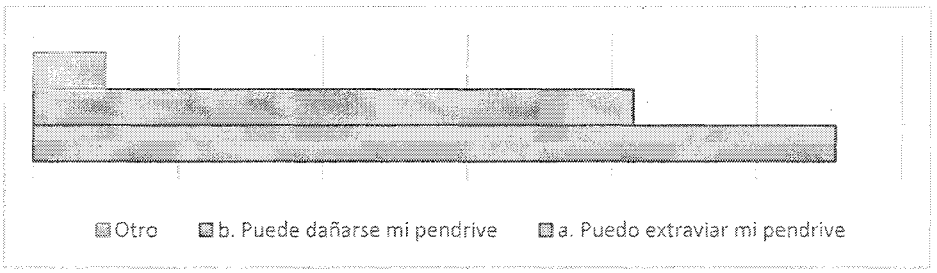


Ilustración 37 Desconfianza en gestor de contraseñas portable

a. Puedo extraviar mi memoria *USB* 89%

b. Puede dañarse mi memoria *USB* 66%

Otro 8%

Cierre

27. ¿En caso de presentarse un estudio el cual arroje resultados más favorables hacia un tipo de Gestor de Contraseñas especifico, estaría dispuesto a utilizar este tipo de Gestor de Contraseñas?

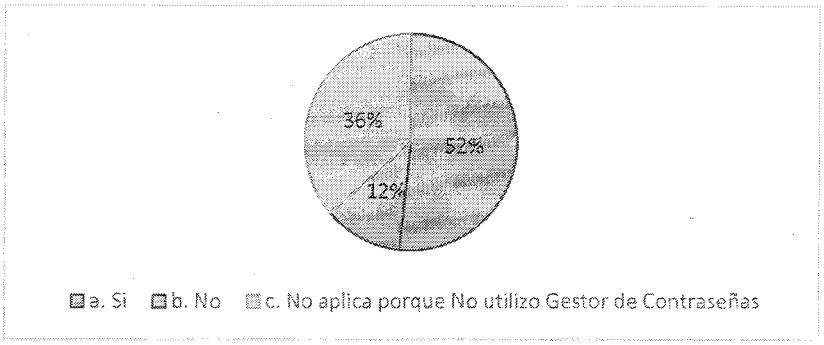


Ilustración 38 Cambio de gestor de contraseñas por resultados del estudio

a. Si	52%
b. No	12%
c. No aplica porque No utilizo Gestor de Contraseñas	36%

Negativo 27.

28. En caso negativo, ¿porque No utilizaría este tipo de Gestor de Contraseñas?

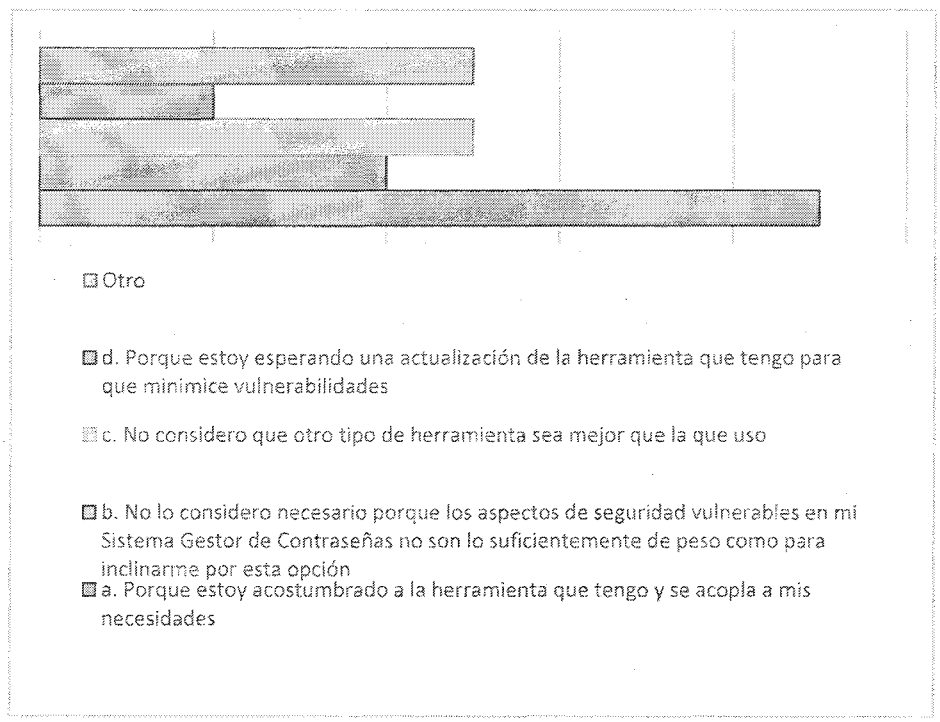


Ilustración 39 Rechazo al cambio de gestor de contraseñas

a. Porque estoy acostumbrado a la herramienta que tengo y se acopla a mis necesidades	41%

b. No lo considero necesario porque los aspectos de seguridad vulnerables en mi Sistema Gestor de Contraseñas no son lo suficientemente de peso como para inclinarme por esta opción	18%
c. No considero que otro tipo de herramienta sea mejor que la que uso	23%
d. Porque estoy esperando una actualización de la herramienta que tengo para que minimice vulnerabilidades	9%
Otro	23%

Encuesta sobre uso de gestores de contraseñas

Muchas gracias por tomarse el tiempo para completar esta encuesta. Su opinión es de gran importancia para realizar un estudio a través del cual se sepa cuál es el grado de conocimiento y uso de los Gestores de Contraseñas en la actualidad.

Esta encuesta requiere sólo unos 10 minutos de su tiempo. Sus respuestas serán totalmente confidenciales y todos los resultados de la encuesta serán utilizados para publicarse en el estudio formal que se está realizando.

Las preguntas marcadas con un asterisco (*) requieren una respuesta obligatoria para avanzar por la encuesta.

Si tiene preguntas acerca de la encuesta, puede contactarme por correo electrónico a mau.ramirez.leguizamon@gmail.com

Para avanzar por esta encuesta, utilice los siguientes botones de navegación de la encuesta:
Haga clic en el botón Siguiente para avanzar a la página siguiente.
Haga clic en el botón Anterior para volver a la página anterior.
Haga clic en el botón Enviar para enviar su encuesta al finalizar todas las preguntas.

Mauricio Andres Ramirez Leguizamon
Estudiante Maestría en Seguridad Informática
Universidad de Buenos Aires

Datos de Participante

A continuación se solicitaran datos para identificar la población que está respondiendo la encuesta:

Es hombre o mujer: *

- Hombre
- Mujer

Elija el rango de edades en el que usted se encuentra: *

- Hasta 20 años
- Más de 20 años y menos de 25 años
- Más de 25 años y menos de 30 años
- Más de 30 años y menos de 40 años
- Más de 40 años
- Otros:

Indique el grado máximo de formación académica que posee: *

- Secundaria
- Universitaria
- Especialización
- Maestría
- Doctorado
- Otros:

Indique su país de residencia actualmente: *

- Colombia
- Argentina
- Chile
- Canadá
- Perú
- Venezuela
- Otros:

Indique el área en que se desempeña laboralmente: *

- Tecnología/Sistemas/IT
- Marketing y Publicidad
- Administración y Contabilidad
- Finanzas/Economía

- Operación del negocio
- Salud
- Recursos humanos
- Recepción/Secretaria/Atención al cliente
- Comercial/Ventas
- Diseño Grafico
- Arquitectura
- Educación
- Diseño electrónico/eléctrico
- Otros:

Indique la jerarquía del puesto en el que se desempeña: *

- Director
- Jefe/Supervisor/Responsable
- Senior
- Semi-senior
- Junior
- Practicante
- Otros:

Generalidades

1. ¿Utiliza más de un servicio que requiera inicio de sesión a través de Internet? *

(Correos electrónicos, chats, servicios de bancos, redes sociales, bolsas de empleo, periódico, etc.)

a. Si

b. No

2. ¿Qué servicios? *

a. Gmail

b. Yahoo

c. Outlook

d. Homebanking

e. Youtube

f. Skype

g. Facebook

h. Twitter

i. Zonajobs

Otros:

3. En su opinión, ¿las contraseñas que utiliza para acceder a esos servicios *son* apropiadas? *

a. Si

b. No

4. ¿Las contraseñas que utiliza tienen una longitud mayor a 8 caracteres? *

a. Si

b. No

5. ¿Las contraseñas que utiliza son de fácil asociación a documentos, información dependiente de usted o email? *

(DNI, Pasaporte, Teléfono, correo electrónico)

a. Si

b. No

6. ¿Utiliza combinaciones de letras con números y caracteres especiales para crear sus contraseñas? *

a. Si

b. No

7. Cuando cambia de contraseña, ¿esta difiere de la anterior notoriamente? *

a. Si. Difieren completamente.

b. No. Conservo algo en particular de la contraseña anterior para recordarla fácilmente.

8. ¿Alguna vez ha olvidado una contraseña? *

a. Si

b. No

9. ¿Utiliza la misma contraseña o alguna parecida para más de un servicio? *

a. Si

b. No

10. ¿Cada cuánto cambia sus contraseñas? *

a. De 1 a 3 meses

b. De 3 a 6 meses

c. De 6 a 12 meses

d. Cada vez que la aplicación me lo solicita

e. Nunca la(s) cambio

11. ¿Usa una frase de contraseña (PASSPHRASE) para definir la contraseña? *

Ejemplo: Frase--> La Vida Es Bella, Contraseña--> LVEB

a. Si

b. No

12. ¿Cómo administra sus contraseñas? *

a. Memorizándolas

b. En físico (por ejemplo en una libreta de anotaciones)

c. En un archivo de texto (en el computador o Celular)

d. En un sistema gestor de contraseñas (Un Sistema Gestor de Contraseñas es un software o servicio que se encarga de administrar/almacenar la información de autenticación del usuario (generalmente id de usuario y contraseña) ya sea en la nube o localmente)

e. Memorizándolas y en físico

f. Memorizándolas y en archivo de texto

g. Memorizándolas y en Sistema Gestor de Contraseñas

h. Memorizándolas, en físico y en un archivo de texto

i. Memorizándolas, en físico y en Sistema Gestor de Contraseñas

j. En físico y en archivo de texto

k. En físico y en Sistema Gestor de Contraseñas

l. En físico, en archivo de texto y en Sistema Gestor de Contraseñas

m. En archivo de texto y en Sistema Gestor de Contraseñas

n. Memorizándolas, en físico, en un archivo de texto y en un Sistema Gestor de Contraseñas

Otros:

Sistemas de Gestión de Contraseñas

Un Sistema Gestor de Contraseñas es un software o servicio que se encarga de administrar/almacenar la información de autenticación del usuario (generalmente id de usuario y contraseña) ya sea en la nube o localmente.

13. ¿Qué Gestor de Contraseñas utiliza? *

a. *ROBOFORM*

b. *KeePass*

c. *LastPass*

d. Password Safe

e. Lockcrypt

f. Password Memory

Otros:

14. ¿Porque utiliza este Gestor de Contraseñas? *

a. Me lo recomendó un amigo

b. Estaba bien calificado en una publicación

c. En mi empresa se maneja esta solución

d. Fue la mejor opción que investigue y se adecua a mis necesidades

e. No conozco otra opción

Otros:

15. ¿Qué características conoce brinda el Gestor de Contraseñas que utiliza actualmente?

a. Autocompletado

b. *MASTER PASSWORD*

c. Multiplataforma

d. Criptografía de datos

e. Disponibilidad en cualquier parte desde la nube

16. ¿Porque lo considera apropiado para sus necesidades? *

a. Es fácil de usar

b. Garantiza que mis datos no serán modificados y/o alterados

c. Es práctico

d. Garantiza Privacidad de mis datos

e. Puedo llevar a todo lado los datos conmigo

Otros:

17. ¿En caso de pérdida o daño de su PC/Celular (donde se estén guardando los datos), o falta de acceso al servicio que tenga en la nube, tiene una copia de respaldo de la información? *

a. Si

b. No

Positivo 17.

18. ¿Cómo conserva su copia de respaldo? *

a. Copia de seguridad en otro PC/celular

b. Copia de seguridad en otro medio de almacenamiento

c. Copia de seguridad física escrita

d. Copia de seguridad en la nube

Otros:

Satisfacción con la elección

19. ¿Está satisfecho con la elección de su Gestor de Contraseñas? *

a. Si. Mi solución es completa.

b. No. Podría mejorar si ofreciera características adicionales.

Negativo 19.

20. ¿Qué característica(s) adicional(es) le hace(n) falta a su Gestor de Contraseñas? *

a. *MASTER PASSWORD*

b. Autocompletado

c. Acceso desde cualquier parte

d. Almacenamiento de datos localmente

e. Exportación de datos

f. Tener los datos únicamente conmigo (en una memoria *USB*)

Tipos de Sistemas Gestores de Contraseñas

Gestor de Contraseñas Local

Un Gestor de Contraseñas local es un software que se instala en un equipo y que permite guardar datos de usuario (id de usuario y contraseña por ejemplo). Los datos que almacena permanecen en el disco o memoria del equipo.

21. ¿Considera seguro delegar id de usuario y contraseña a un Gestor de Contraseñas local? *

a. Si

b. No

Negativo 21.

22. En caso negativo ¿porque?

a. Mi maquina puede ser vulnerada y se pueden hacer con mis datos

b. Mi maquina puede dañarse y toda la información en ella también

c. Mi maquina es de uso compartido

Otros:

Gestor de Contraseñas Online

Un Gestor de Contraseñas online es un servicio en la nube que se presta para almacenar datos de usuario (id de usuario y contraseña por ejemplo). Los datos residen en los servidores de la empresa que presta el servicio (guarda los datos)

23. ¿Considera seguro delegar id de usuario y contraseña a un Gestor de Contraseñas online? *

a. Si

b. No

Negativo 23.

24. En caso Negativo, ¿porque?

a. No confío en que terceros tengan mis datos

b. Prefiero conservar los datos yo mismo

c. No confío en los mecanismos de Criptografía actuales del mercado

Otros:

Gestor de Contraseñas Portable

Un Gestor de Contraseñas Portable es un software para almacenar datos de usuario (id de usuario y contraseña por ejemplo) el cual se instala en una memoria *USB* o disco externo. Los datos residen en la memoria *USB* o disco externo.

25. ¿Considera seguro delegar id de usuario y contraseña a un Gestor de Contraseñas Portable? *

a. Si

b. No

Negativo 25.

26. En caso negativo, ¿porque?

a. Puedo extraviar mi memoria *USB*

b. Puede dañarse mi memoria *USB*

Otros:

Cierre

27. ¿En caso de presentarse un estudio el cual arroje resultados más favorables hacia un tipo de Gestor de Contraseñas especifico, estaría dispuesto a utilizar este tipo de Gestor de Contraseñas?*

a. Si

b. No

c. No aplica porque No utilizo Gestor de Contraseñas

Negativo 27.

28. En caso negativo, ¿porque No utilizaría este tipo de Gestor de Contraseñas?*

a. Porque estoy acostumbrado a la herramienta que tengo y se acopla a mis necesidades

b. No lo considero necesario porque los aspectos de seguridad vulnerables en mi Sistema Gestor de Contraseñas no son lo suficientemente de peso como para inclinarme por esta opción

c. No considero que otro tipo de herramienta sea mejor que la que uso

d. Porque estoy esperando una actualización de la herramienta que tengo para que minimice vulnerabilidades

Otros:

Gracias!!!

Cualquier comentario adicional en relación al tema puede dejarlo a continuación

Anexo II: INSTALACIÓN Y PRESTACIONES DE LOS GESTORES DE CONTRASEÑAS ANALIZADOS

Para este trabajo se creó un ambiente en VMWare Workstation 10 en tres máquinas virtuales denominadas A, B y C respectivamente, con *Windows* 7 home Premium, en una sesión con permisos administrativos, sin actualizaciones de seguridad, sin antivirus y con las aplicaciones objeto de este trabajo, las cuales son *LastPass* v3.1.65, *KEEPASS2* v 2.28 y *Roboform2Go* V 7.9.9.1. Se utiliza una cuenta de correo en Yahoo real, de la cual se van a almacenar los datos de inicio de sesión en los diferentes sistemas para las demostraciones.

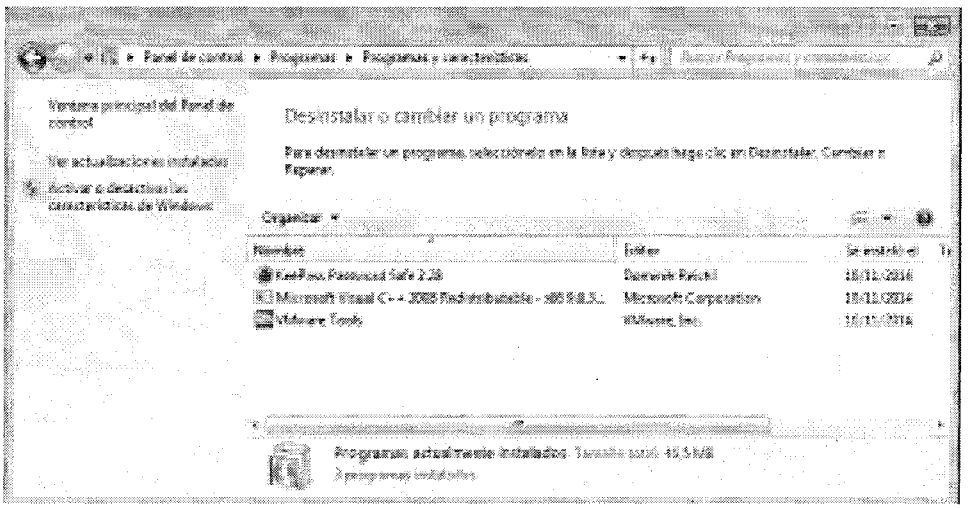


Ilustración 40 Software instalados en máquina virtual A

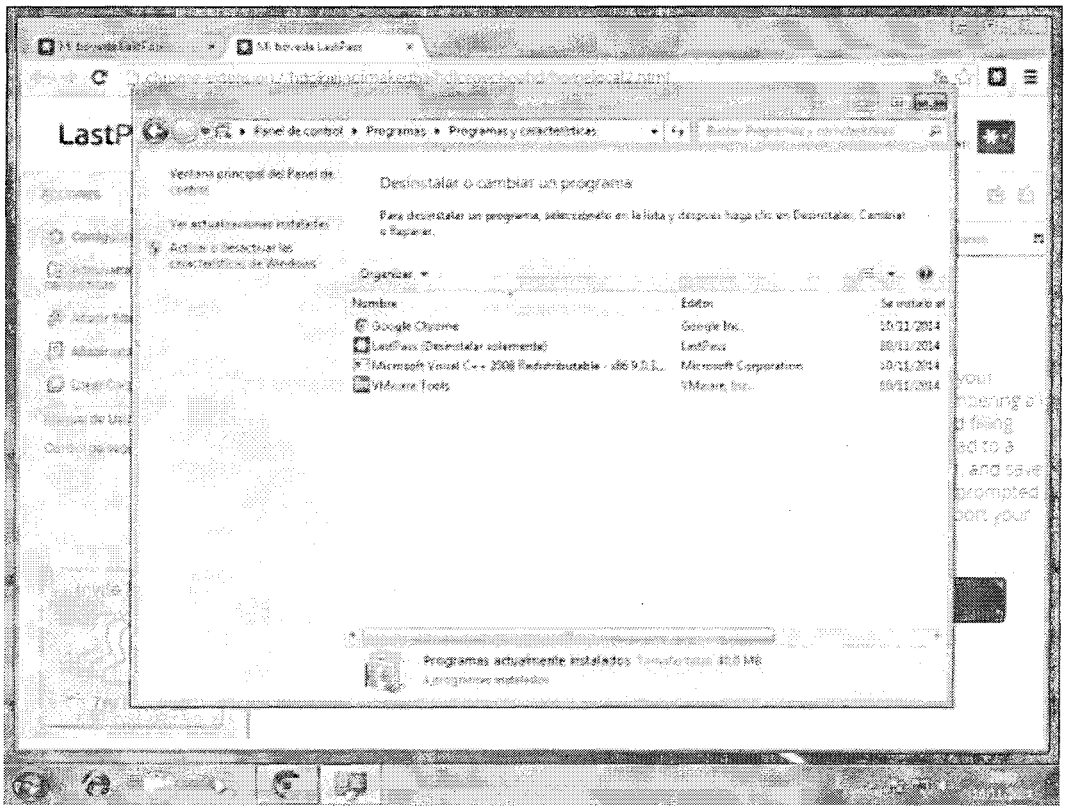


Ilustración 41 Software instalado en maquina B

La máquina C no se representa debido a que va a ser la opción del Gestor de Contraseñas portable y no hace falta instalarlo para visualizarlo en el panel de control.

Gestión de contraseñas en *KEEPASS2*

La versión por defecto solo trae el idioma inglés, si se requiere otro idioma, hay que descargarlo desde la aplicación, la cual hará una búsqueda al sitio de descargas de *KeePass*.

El procedimiento para su configuración se describe a continuación [27]:

1. En primera instancia, se accede a la aplicación correspondiente y cuando es una instalación nueva, se crea una nueva BD:

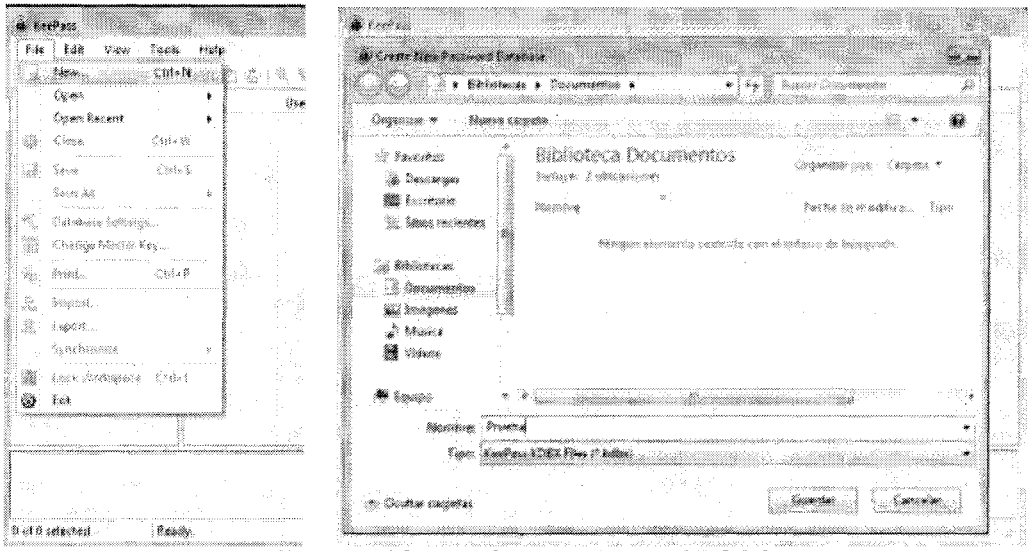


Ilustración 42 Crear BD *KEEPASS2*

2. A continuación se muestra el siguiente menú para configurar:

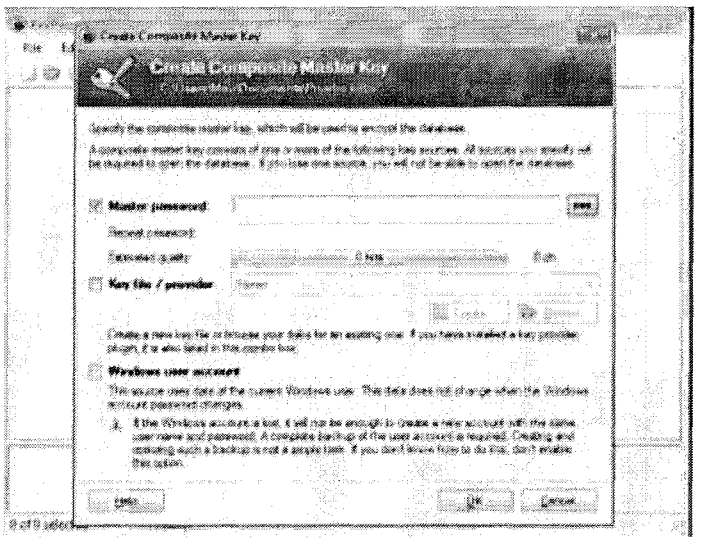


Ilustración 43 Creación MASTER KEY *KeePass*

3. Se escribe una contraseña fuerte, gracias al nivel de calificador que tiene incorporado la herramienta y se elige si se desea utilizar un KEYFILE para adicionar protección, sin este KEYFILE en conjunto con la BD, no se podrá acceder al almacén de datos.

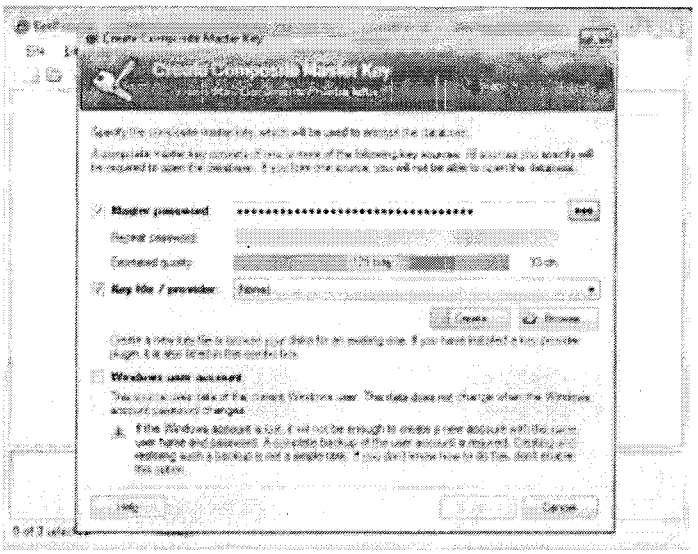


Ilustración 44 Fortaleza de la MASTER KEY

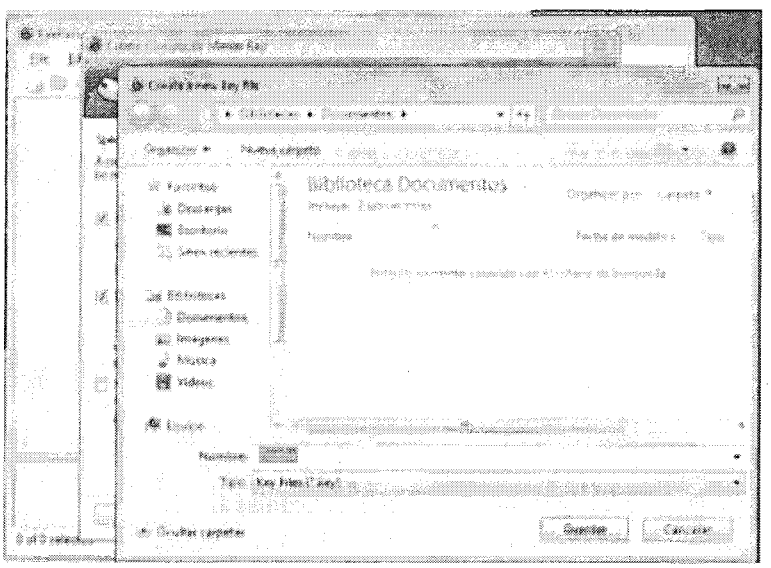


Ilustración 45 Creación KEYFILE

4. A continuación aparece la opción para crear el patrón con el cual se va a generar el KEYFILE. Se ingresa ya sea por el mouse o por el teclado cualquier opción para que el archivo tenga una creación

pseudorandomica.

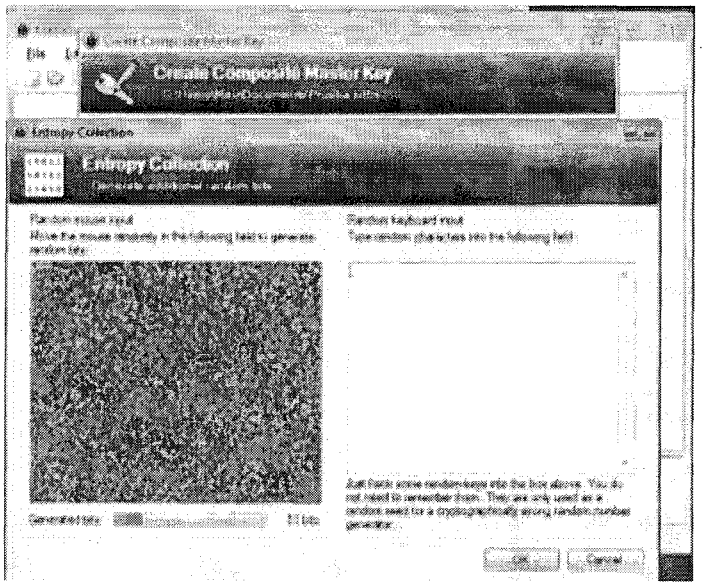


Ilustración 46 Generación pseudorandomica

Nota: La opción de utilización con la cuenta de usuario de *Windows* no será utilizada para esta práctica.

5. Posterior a esto, se avanza al siguiente paso el cual es de configuración de la BD

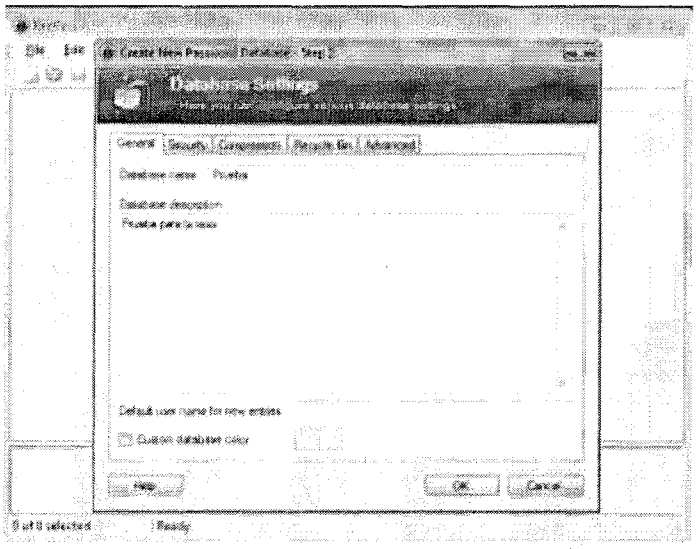


Ilustración 47 Configuración general BD

6. En esta parte se elige la seguridad de la BD: se elige el algoritmo de

criptografía y se configura la transformación del archivo para la prevención de ataques por diccionario o fuerza bruta.

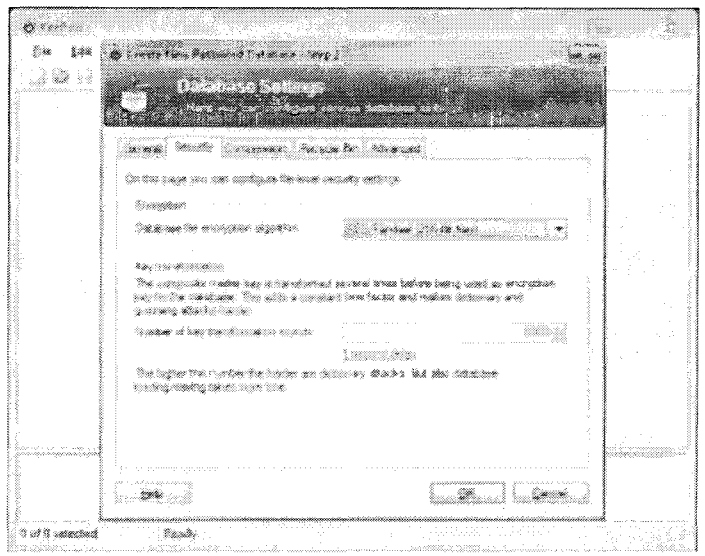


Ilustración 48 Configuración seguridad BD

7. En esta parte se configura la compresión de la BD.

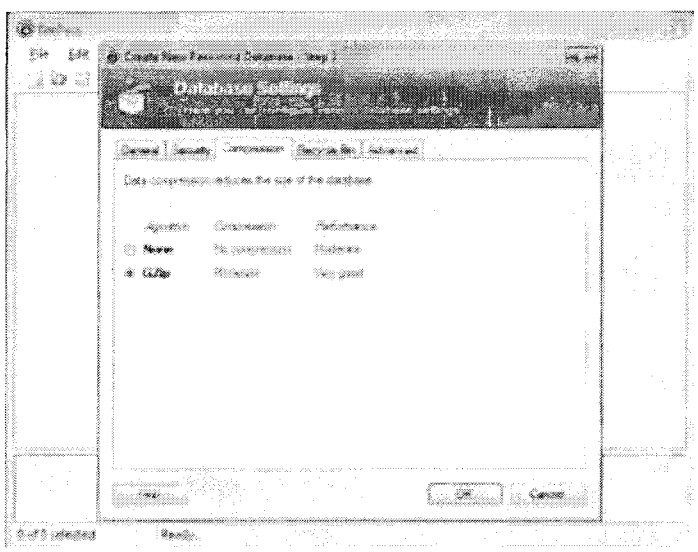


Ilustración 49 Compresión BD

8. En esta opción se configura si la información que se borre vaya a la papelera de reciclaje.

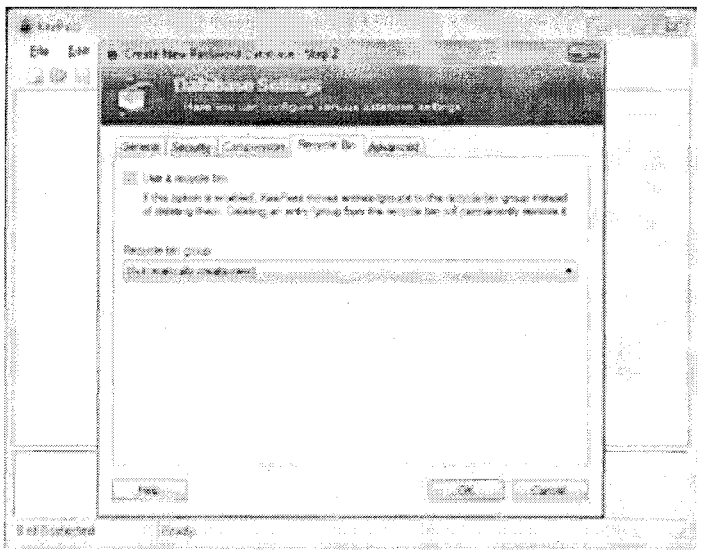


Ilustración 50 Configuración de borrado de información

9. En esta opción principalmente se configura la caducidad y obligatoriedad de la *MASTER PASSWORD* en un periodo determinado de tiempo:

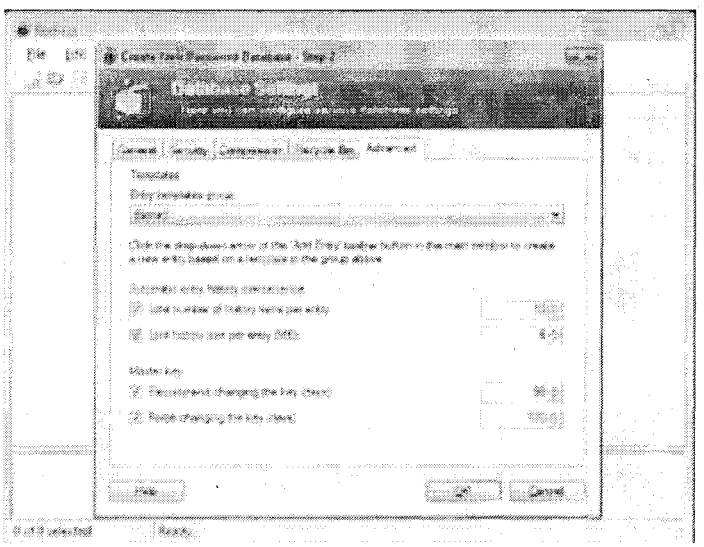


Ilustración 51 Configuración avanzada BD

10. Posteriormente se genera la siguiente vista, donde se crean unos ejemplos de entradas para utilizar la herramienta. A la izquierda se puede ver el nombre de la BD seleccionada y una organización de categorías que se pueden utilizar para organizar los datos.

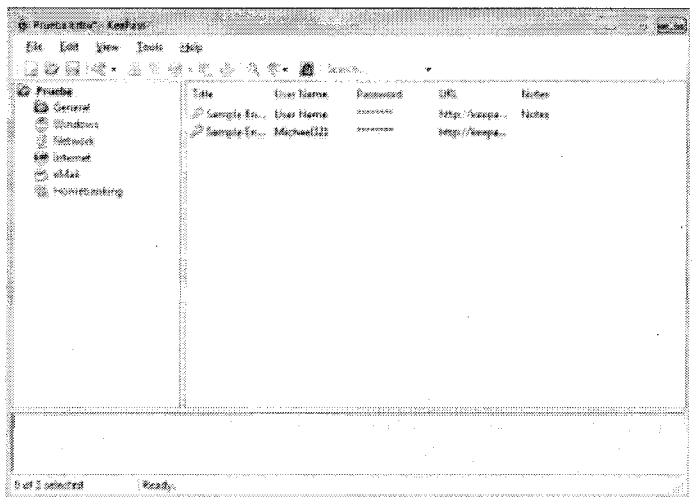


Ilustración 52 Vista de datos

11. Los diferentes menús de la herramienta son los que se muestran a continuación:

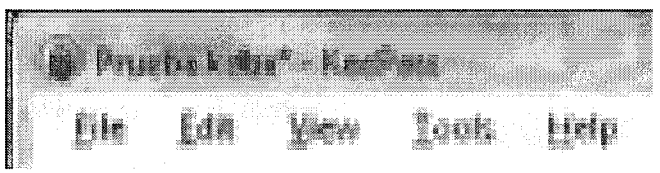


Ilustración 53 Menú *KeePass*

12. En este menú se configuran las entradas que se vayan a generar.

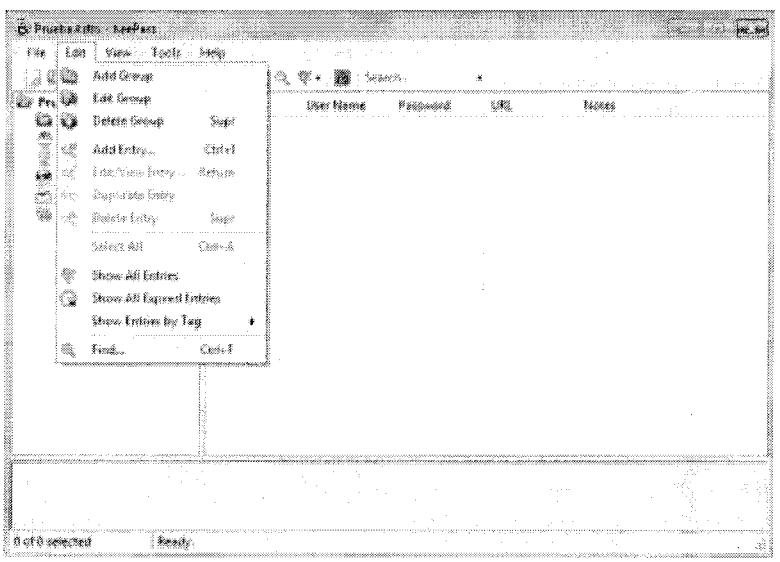


Ilustración 54 Configuración de entradas *KeePass*

13. En la opción de vista se puede configurar la forma en que se van a ver los diferentes paneles de la herramienta.

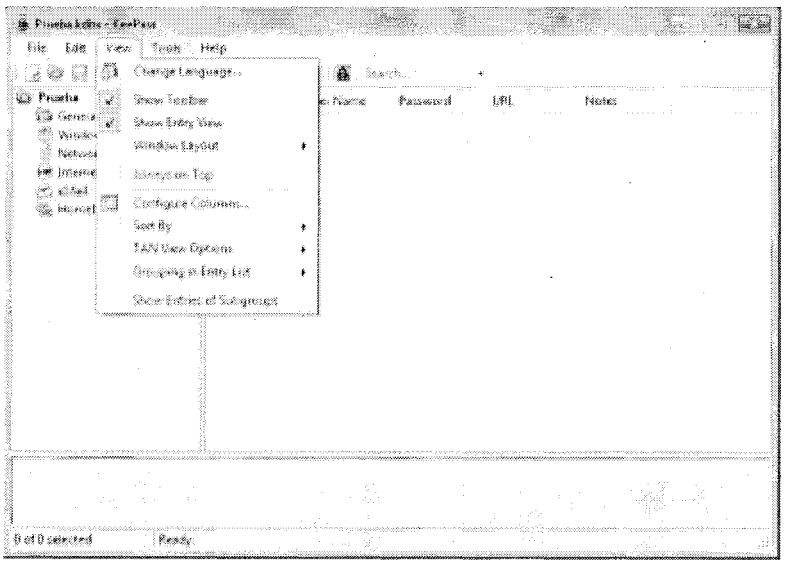


Ilustración 55 Configuración paneles de herramienta

14. En la parte de herramientas se podrán ver las utilidades y la configuración de seguridad que trae la herramienta. Se podrán configurar *PLUGIN*s adicionales que se le quieran instalar a la herramienta y se podrán configurar aspectos de seguridad de la herramienta como las políticas de seguridad que usa.

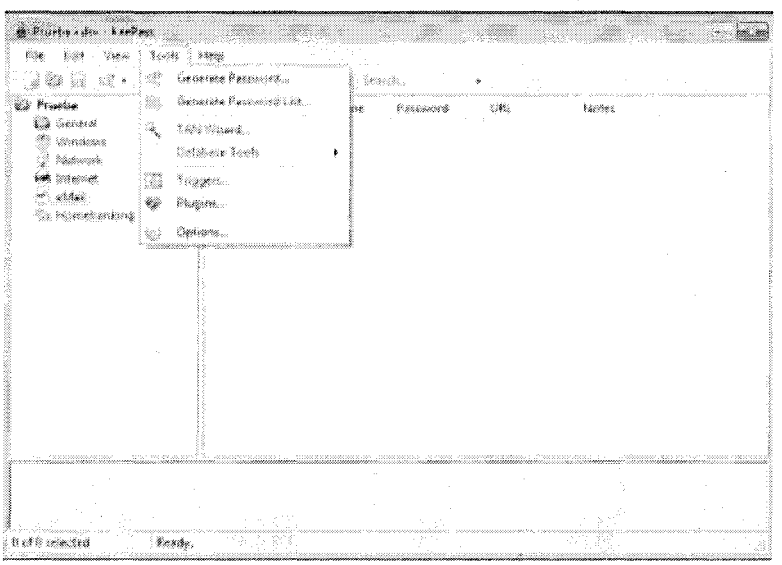


Ilustración 56 Configuración de herramientas *KeePass*

15. En esta opción de seguridad, se puede configurar desde el borrado de la memoria hasta la cantidad de días en que expira una contraseña.

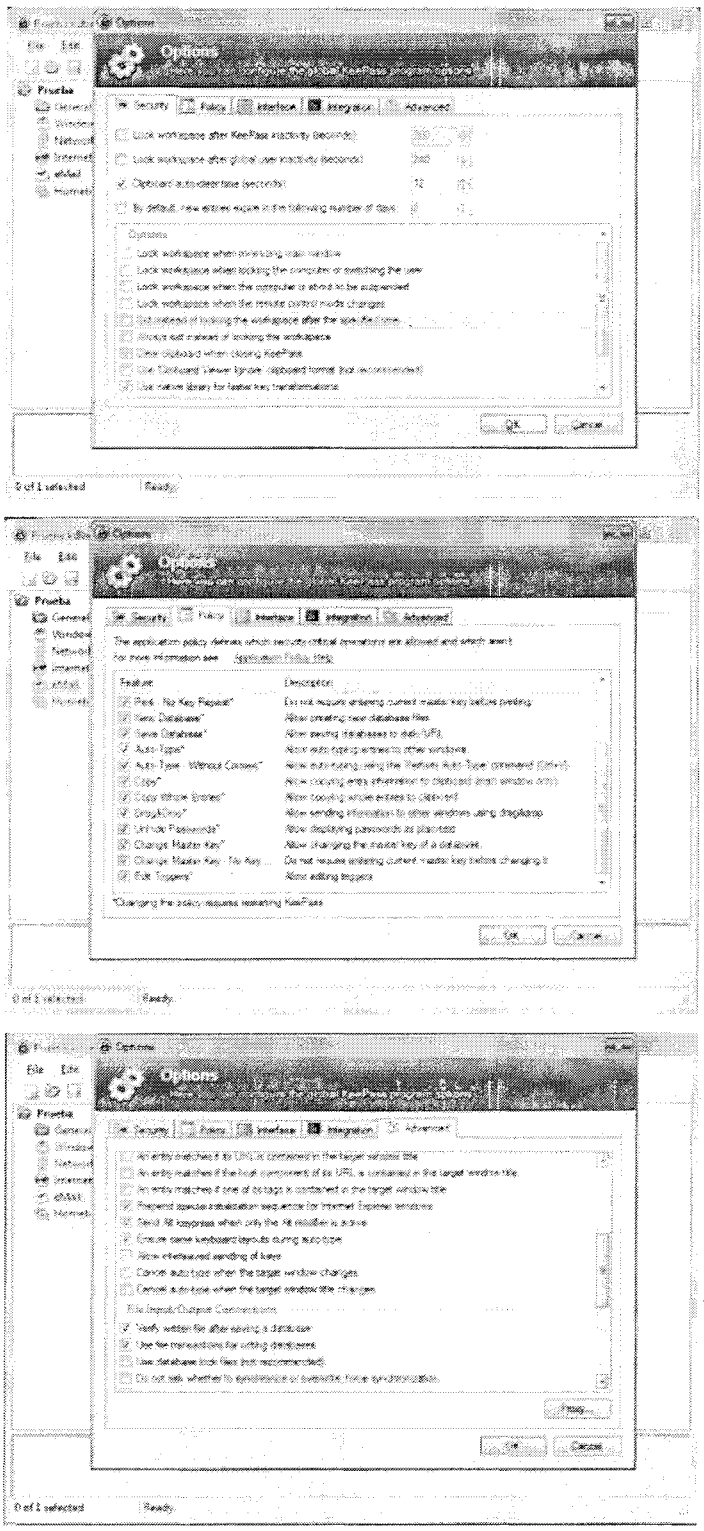


Ilustración 57 Configuración de Opciones

16. Por ultimo está el menú de ayuda que es donde se puede encontrar información técnica de la herramienta y se puede lanzar una búsqueda para encontrar actualizaciones.

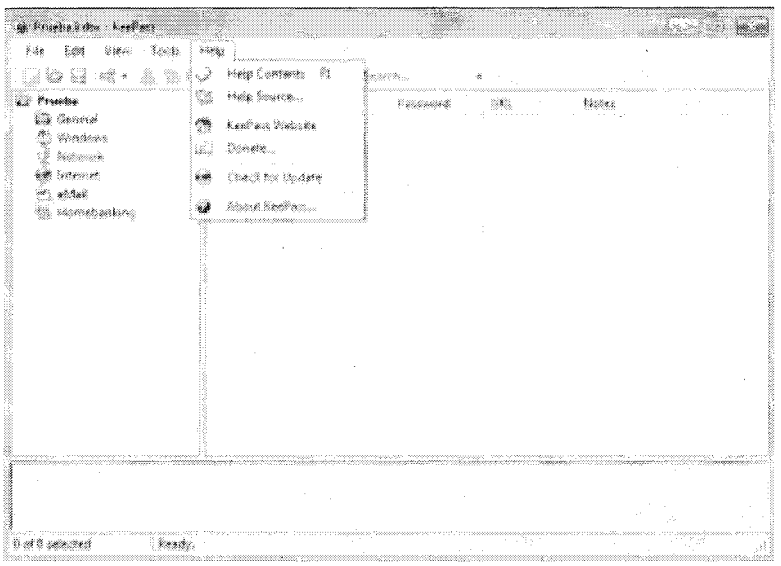


Ilustración 58 Menú de ayuda *KeePass*

Forma de Almacenamiento *KEEPASS2*

En *KEEPASS2* los datos se almacenan en una BD con extensión de archivo *.kdbx la cual esta cifrada con AES o Twofish. Para mayor seguridad se puede configurar un KEYFILE, el cual, si no se logra ubicar, no se podrá acceder a la BD a pesar de tener la *MASTER PASSWORD*.

Los archivos en este caso se almacenaron en el escritorio la BD y en la carpeta de documentos de *Windows* el KEYFILE.

Ilustración 59 Ingreso a *KeePass*

1. Para crear entradas en la herramienta, lo primero es elegir la categoría donde será guardada la información y luego hacer clic derecho en el panel derecho para añadir la entrada:

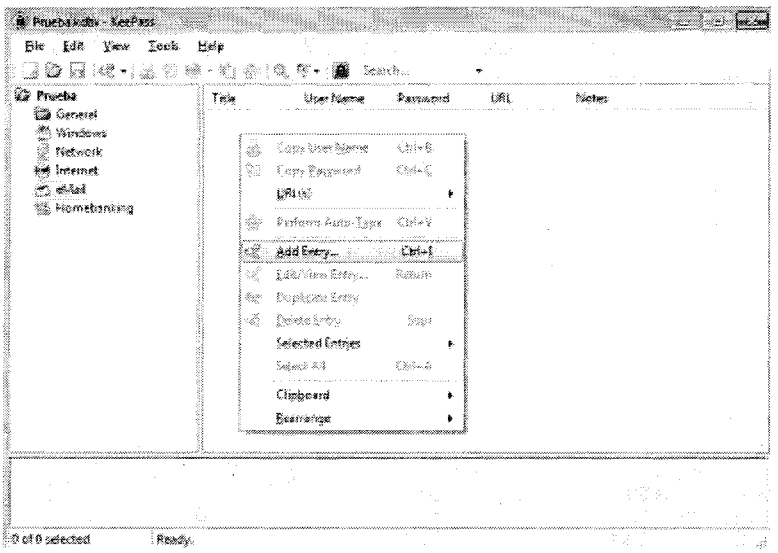
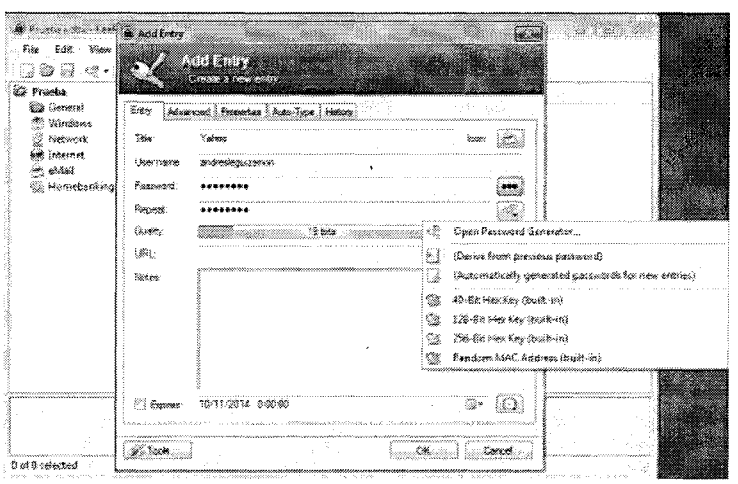
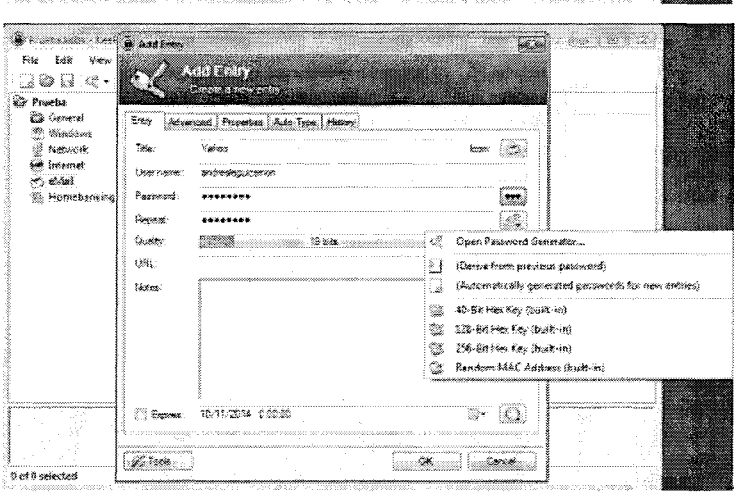


Ilustración 60 Añadir entradas en *KeePass*

2. Después de esto se configura en detalle la entrada, acá se puede elegir desde la generación de la contraseña por medio de la herramienta, hasta la fecha en que esta debiera expirar.





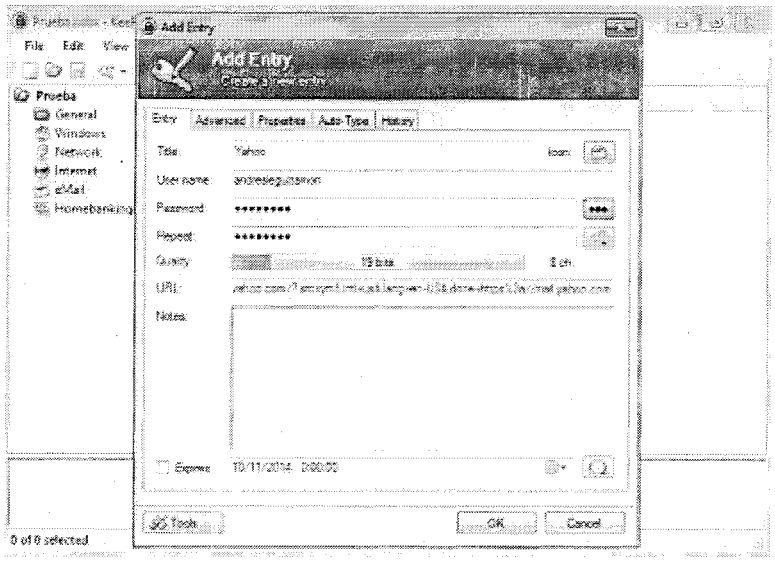
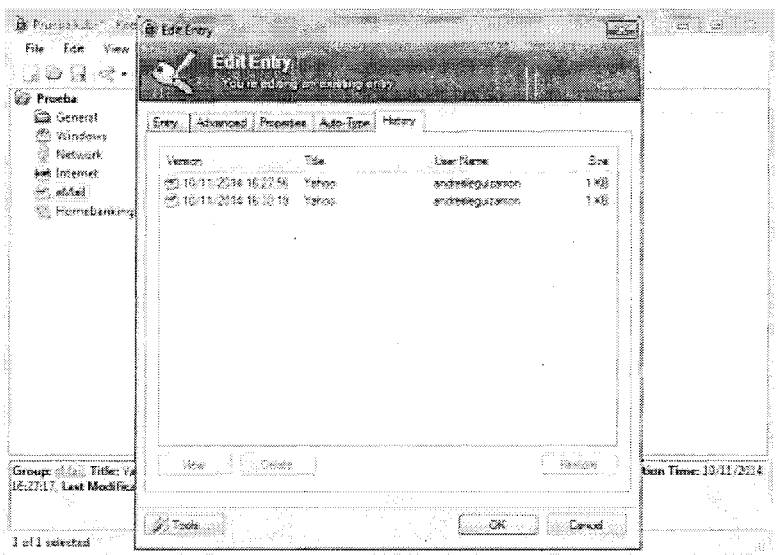


Ilustración 61 Edición entradas en *KeePass*

3. La opción de Historial en la creación de entradas permite tener un nivel de auditoria sencillo para revisar la trazabilidad de la entrada.



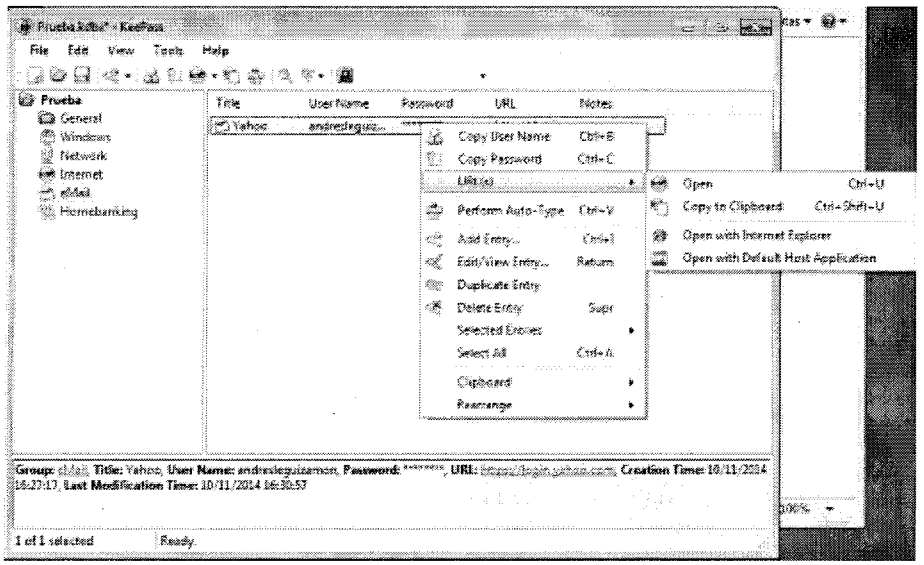


Ilustración 62 Historial creación de entradas

3. La opción de generación de contraseñas funciona de la siguiente forma:

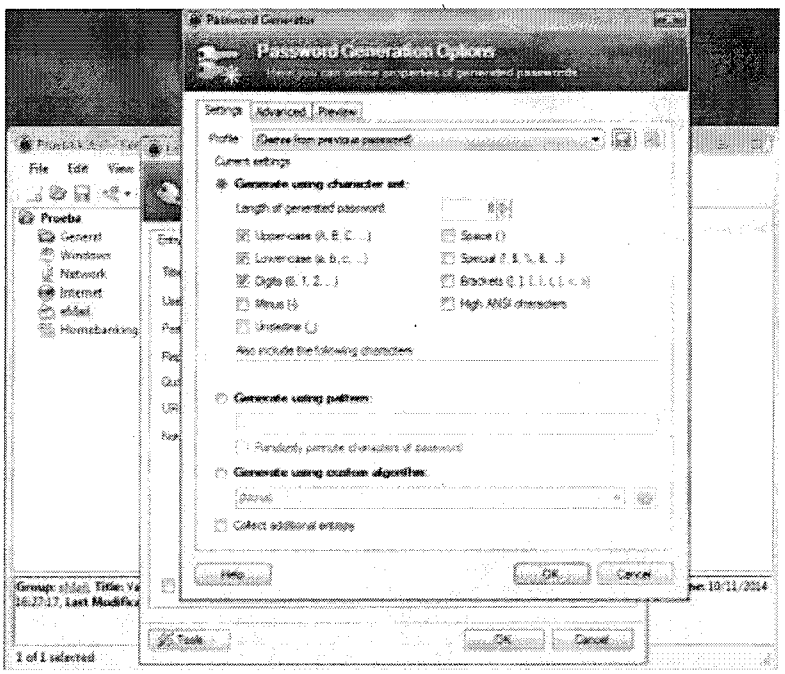


Ilustración 63 Opciones para la generación de contraseñas *KeePass*

De acuerdo a la anterior pestaña se pueden añadir más reglas para la creación de la contraseña.

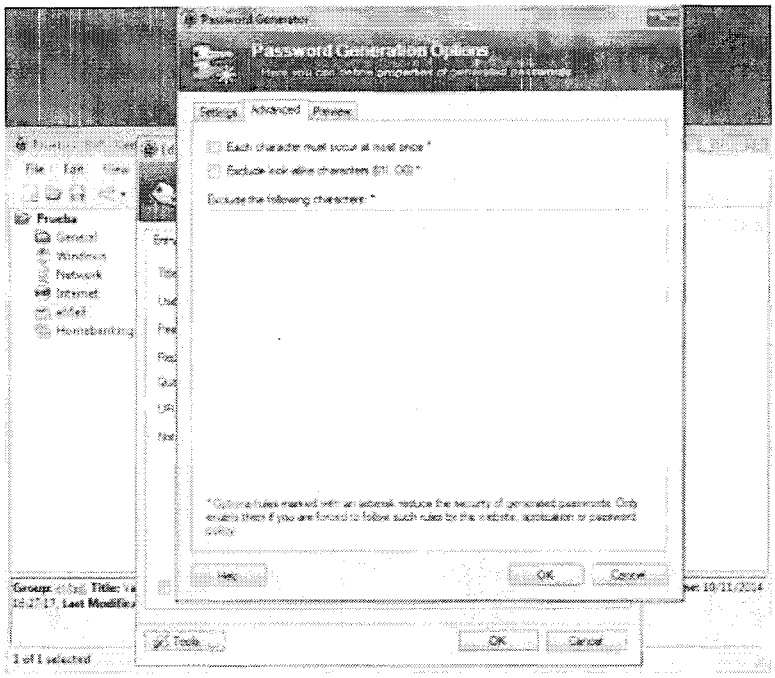


Ilustración 64 Opciones avanzadas para la creación de contraseñas *KeePass*

4. Posteriormente se podrán visualizar las contraseñas que generó la herramienta con base en la configuración anterior elegida.

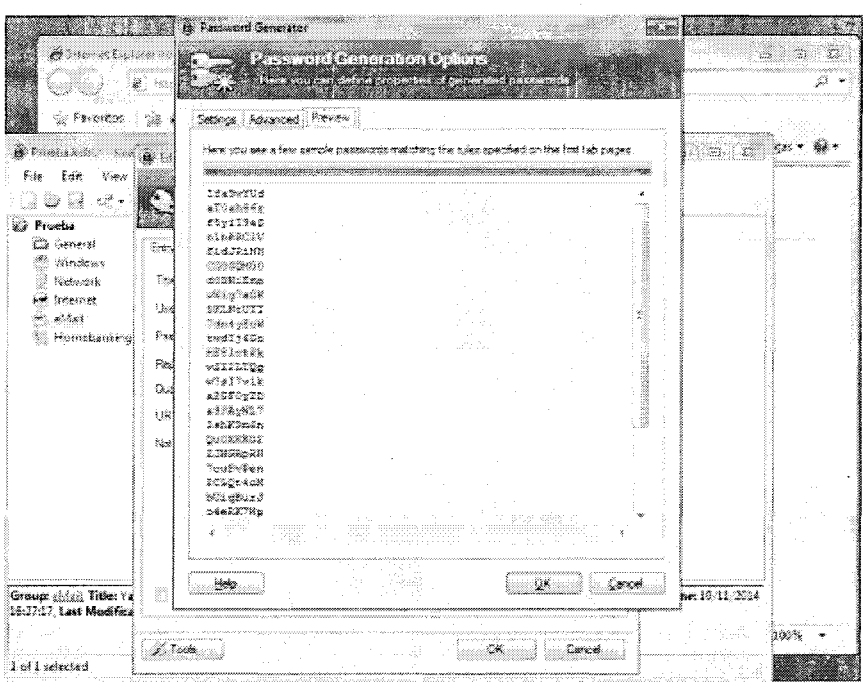


Ilustración 65 Ejemplo de contraseñas autogeneradas *KeePass*

5. La escritura automática se realiza en dos pasos:

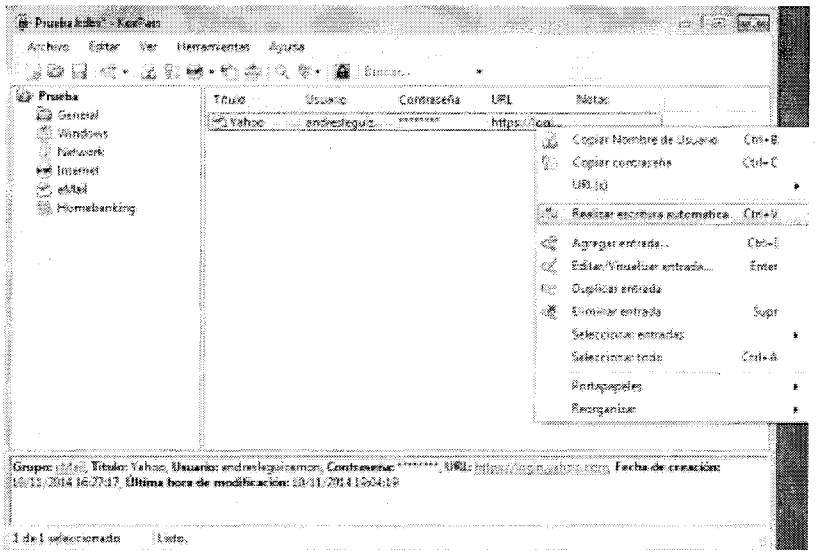


Ilustración 66 Ingreso a las entradas *KeePass*

Primero se abre la *URL* haciendo doble clic en el campo denominado *URL*, posteriormente se abrirá el navegador de internet predeterminado y se accederá a la *URL*. Después desde el navegador se teclea Ctrl + Alt + A que es la combinación de teclas de *KeePass* para disparar la Escritura Automática.

Ilustración 67 Ejemplo de ingreso a Yahoo a través de *KeePass*

Normalmente, la página de *login*, dispone de un formulario con dos cajas de texto, una para introducir el nombre de usuario y otra para introducir

la contraseña. *KeePass* suele detectar correctamente el formulario de entrada y no tiene problemas para introducir el nombre de usuario y la contraseña automáticamente.

En algunos sitios web, la página de *login* no coincide con la página principal del sitio, en tal caso, la *URL* que debe ser almacenada en *KeePass* es la *URL* de la página de *login*.

El autocompletado consiste en la detección de dos cajas de texto para introducción de datos, normalmente son detectados por la herramienta, sin embargo existe la posibilidad que la *URL* almacenada sea la principal del sitio y no coincida con la *URL* de *login*, en este caso hay que predeterminar siempre la de *login*. Para las páginas cuyos campos tienen más de 2 cajas de texto, razón por la cual podría confundirse la herramienta, *KeePass* tiene la opción de configurar manualmente las entradas y los campos correspondientes de una página.

Esto supone un nivel de complejidad mayor para lo que fuera un usuario estándar por ejemplo. Por otro lado, para un usuario avanzado propone mayor nivel de configuración y ajuste a una configuración de seguridad más robusta.

Por ultimo una característica interesante de *KeePass* es que utiliza una doble técnica de envío de pulsaciones de teclas junto con la utilización del portapapeles, de forma que al realizar Escritura Automática, si el computador tiene algún software para capturar pulsaciones del teclado (KEYLOGGERs por ejemplo), es capaz de despistarlo. Esto es bastante útil en computadores de uso público como cybercafes y demás.

El procedimiento para su configuración se describe a continuación [28]:

1. En la instalación de la herramienta aparece automáticamente la opción de descargar los complementos que se instalaran o no en los navegadores que se tengan instalados en el equipo.

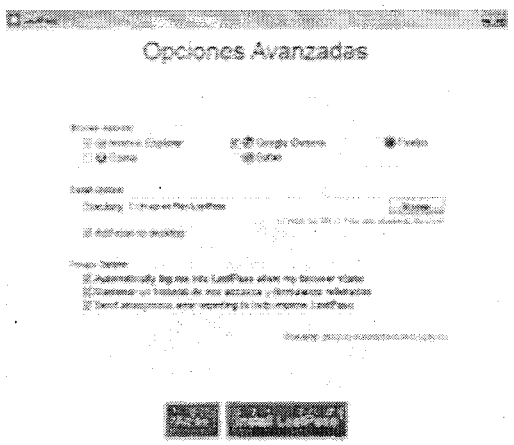


Ilustración 68 Opciones de instalación *LastPass*

2. Para poder utilizar el servicio, al ser un gestor de contraseñas online, hay que generar una cuenta con *LastPass* la cual será la encargada de asociar los datos que se le introduzcan.

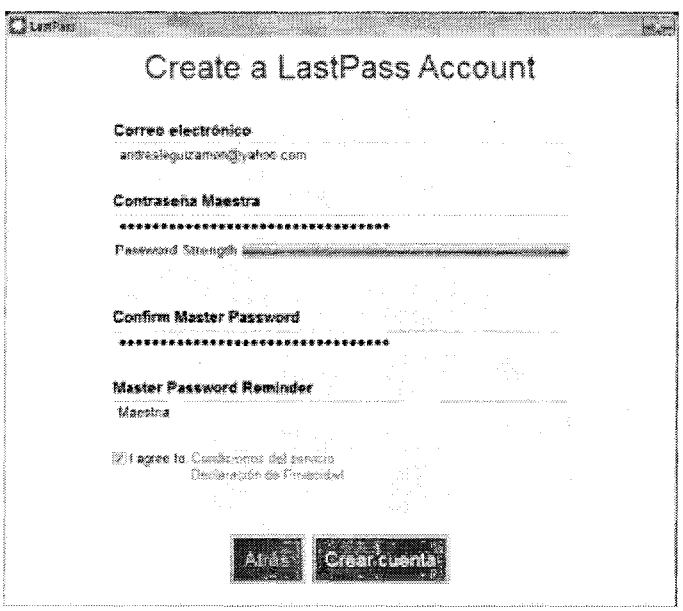
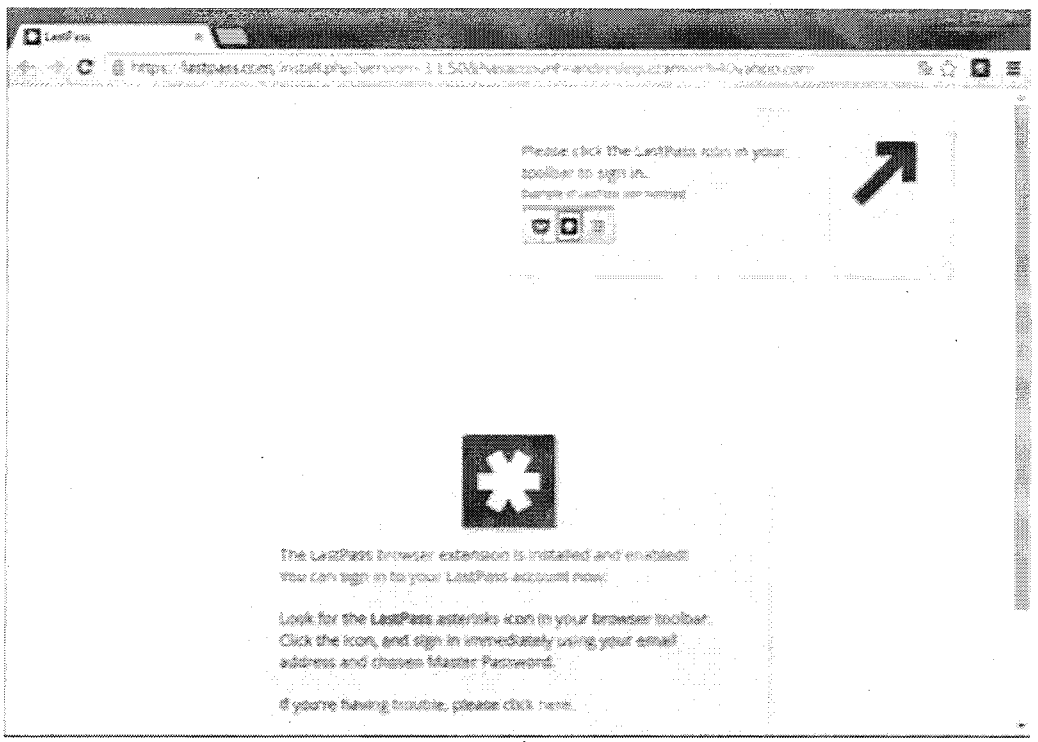


Ilustración 69 Generación de cuenta de usuario *LastPass*



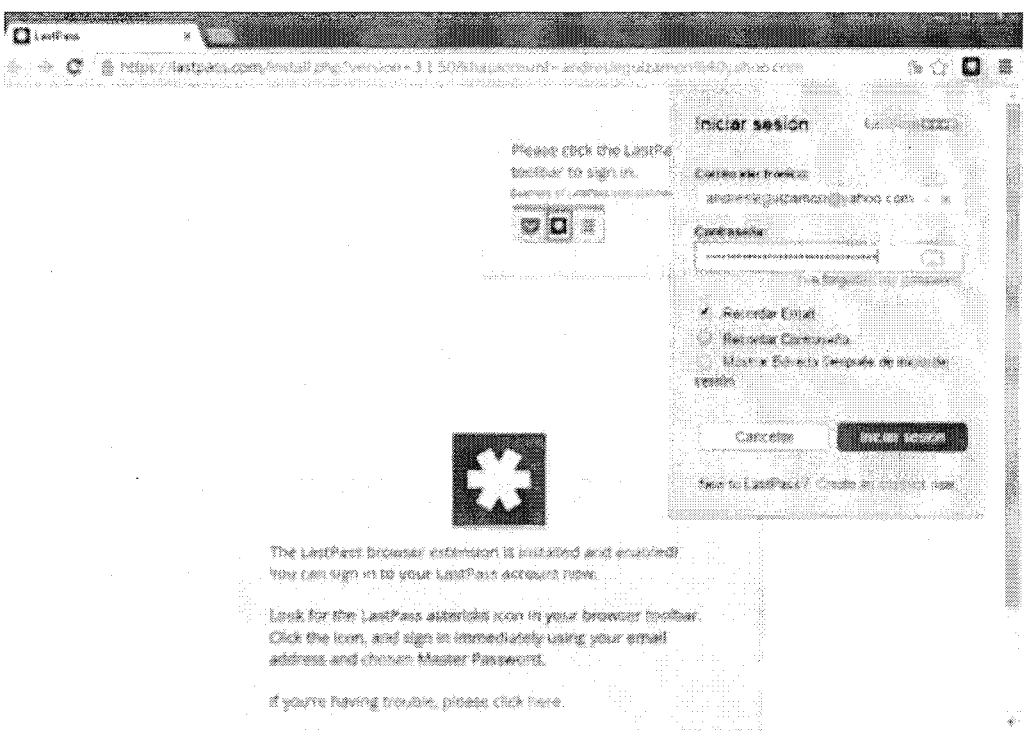


Ilustración 70 Instalación de complemento a navegador de *LastPass*

3. En la pestaña de configuración se puede ver la siguiente información:

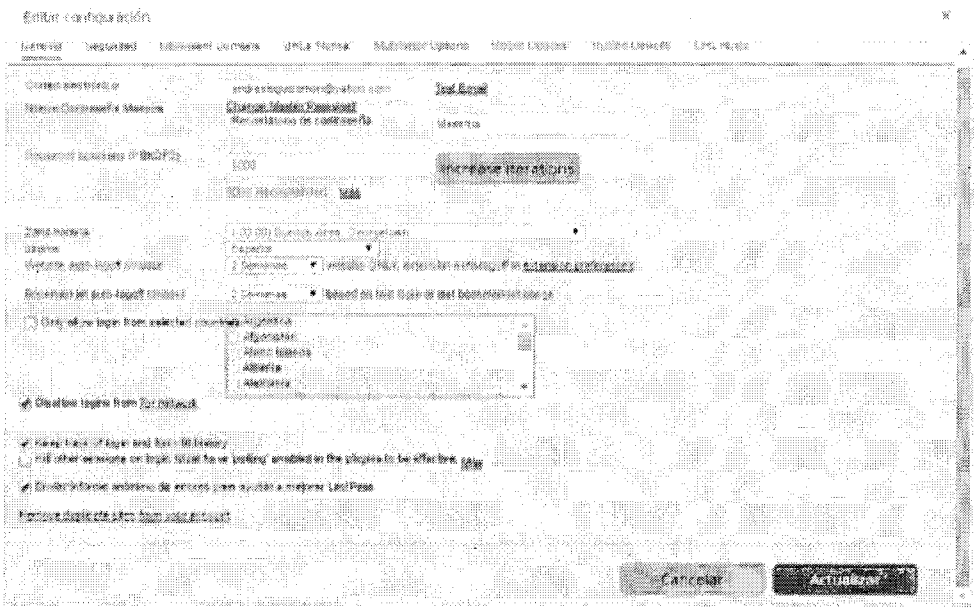


Ilustración 71 Configuración general de *LastPass*

Una característica por la que sobresale *LastPass* es porque utiliza una herramienta denominada PBKDF2, la cual sirve para proteger de ataques de fuerza bruta y de diccionario la *MASTER PASSWORD*. Cada vez que hay que hacer un cambio en la configuración de seguridad de *LastPass* se requiere la *MASTER PASSWORD*, esto con el fin de proteger los datos de usuario.

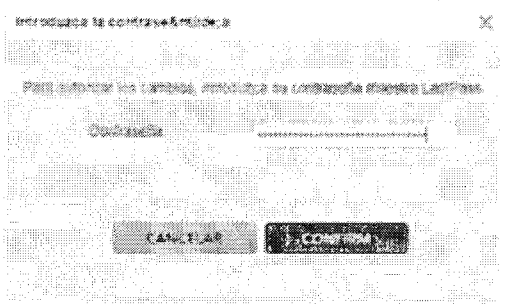


Ilustración 72 Solicitud *MASTER PASSWORD* para ingreso a *LastPass*

La configuración de la seguridad se puede parametrizar de acuerdo a tres niveles de confianza que establece el software:

- Normal: permite revertir cambios del *MASTER PASSWORD*

Solicitar *MASTER PASSWORD* cuando haya que hacer cambios de identidades o gestionar roles

- Media alta: permite revertir cambios del *MASTER PASSWORD*

Solicitar *MASTER PASSWORD* cuando haya que hacer cambios de identidades o gestionar roles

Visualizar o copiar contraseñas

Editar notas seguras

- Alta: permite revertir cambios del *MASTER PASSWORD*

Solicitar *MASTER PASSWORD* cuando haya que hacer cambios de identidades o gestionar roles

Visualizar o copiar contraseñas

Editar notas seguras

Acceder a un sitio

Rellenar o editar el formulario

Ver o editar el sitio

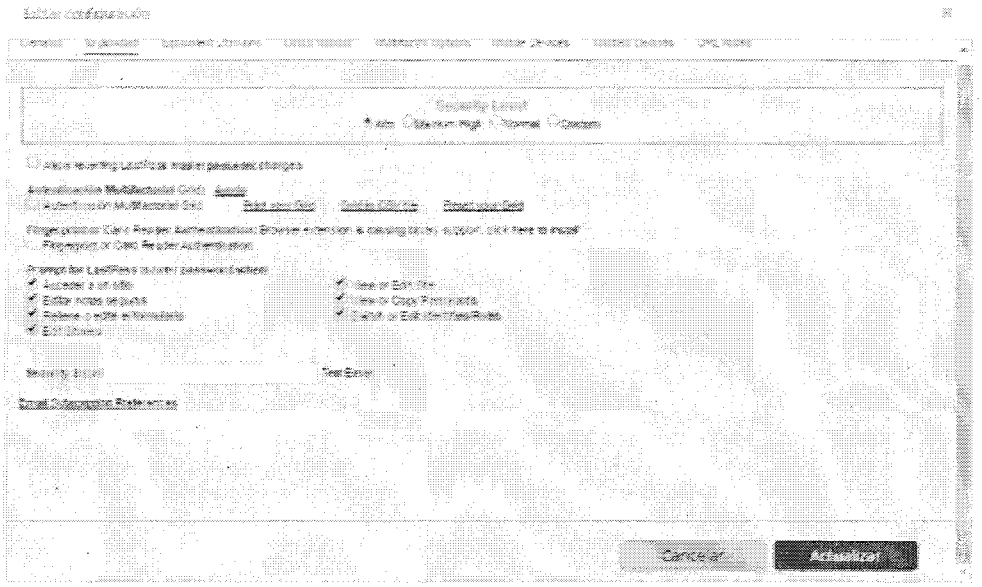


Ilustración 73 Niveles de configuración de seguridad *LastPass*

4. En esta parte de la configuración se activa la autenticación de doble factor por defecto, que es una tarjeta de coordenadas:

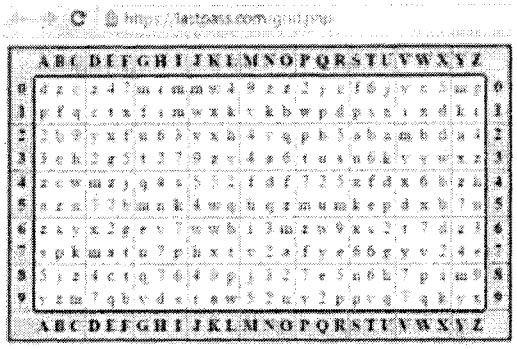


Ilustración 74 Generación de tarjeta de coordenadas *LastPass*

5. Posterior a esto, se solicitara cada vez que aparezca la ventana para ingresar la *MASTER PASSWORD*, una identificación parecida a la tarjeta de coordenadas que se utiliza en los bancos.

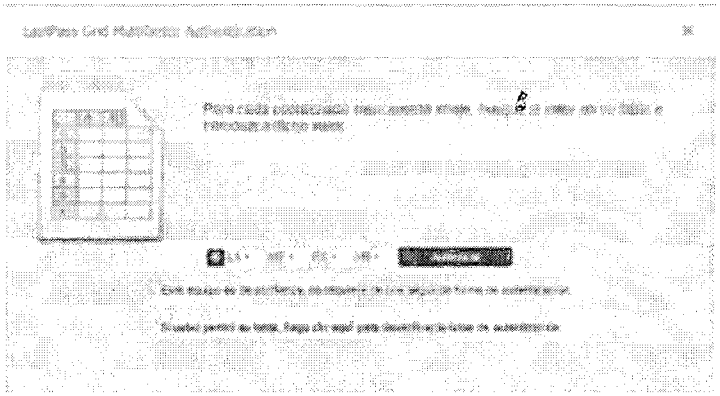


Ilustración 75 Uso de tarjeta de coordenadas *LastPass*

Si se intenta evadir este sistema de doble factor de autenticación, se enviara un correo de seguridad a la cuenta de correo asociada para lograr verificar la identificación y poder recuperar el acceso a la cuenta de *LastPass*:

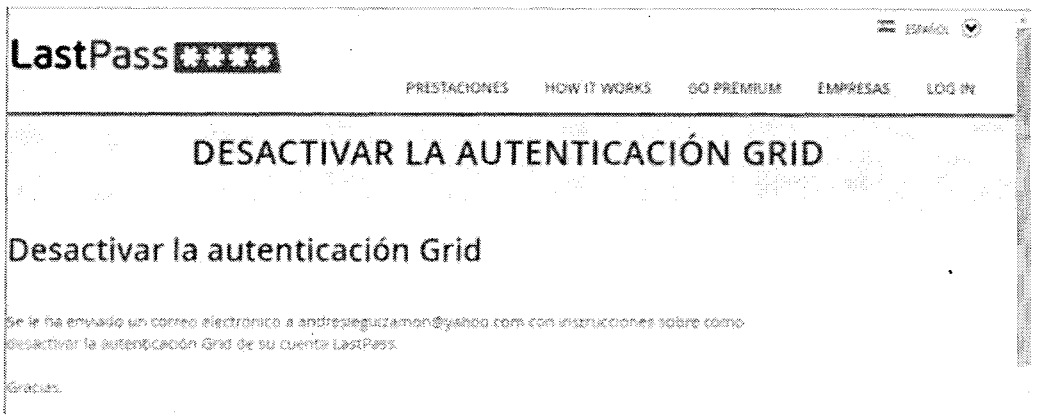


Ilustración 76 Desactivación de tarjeta de coordenadas *LastPass*

Si por error la cuenta asociada fue generada con una secuencia pseudoaleatoria de caracteres, puede complicarse la recuperación de la cuenta de *LastPass*.

6. Adicionalmente existe la opción de configurar las *URL*s a las cuales no debería poder accederse.

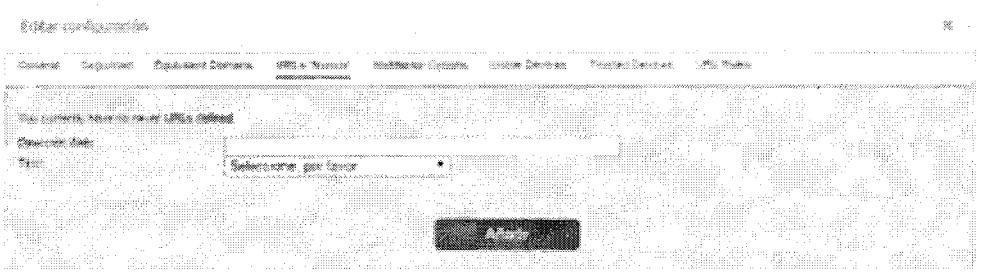


Ilustración 77 Configuración *URL*s de acceso

Las opciones de autenticación de doble factor a través de una aplicación de terceros son yubitkey, google, toopher, seguridad duo y transakt.

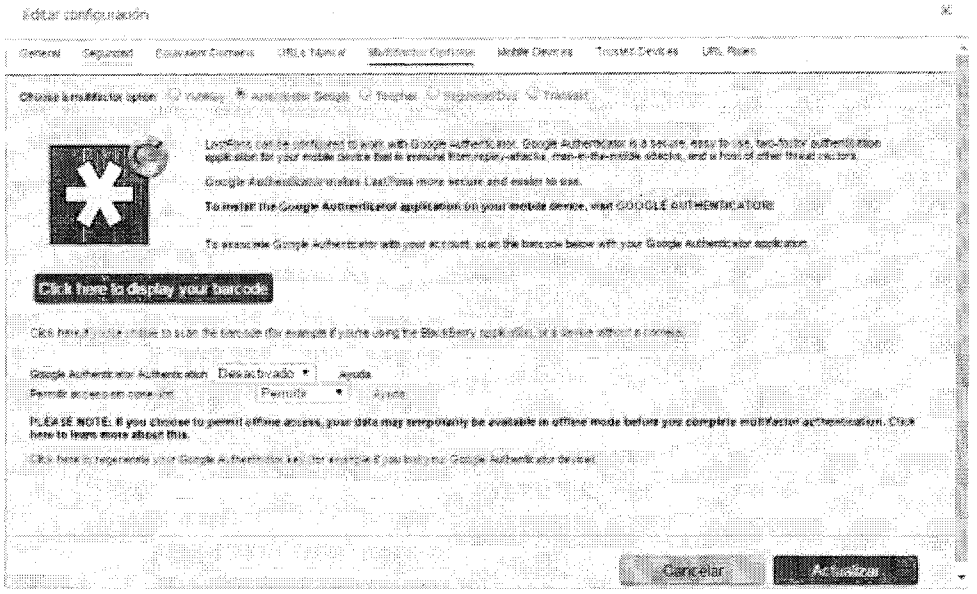


Ilustración 78 Opciones de acceso de doble factor *LastPass*

7. A continuación se verifica la información de certificado que se proporciona a través del navegador:

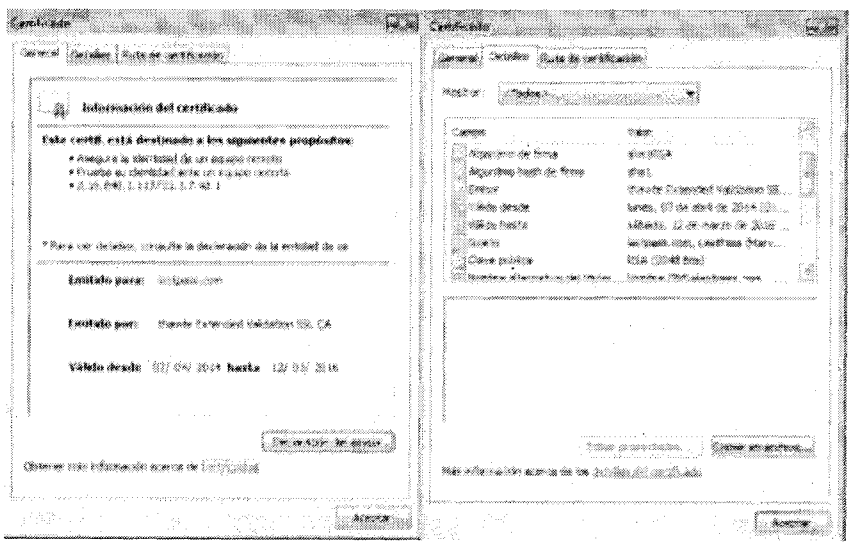
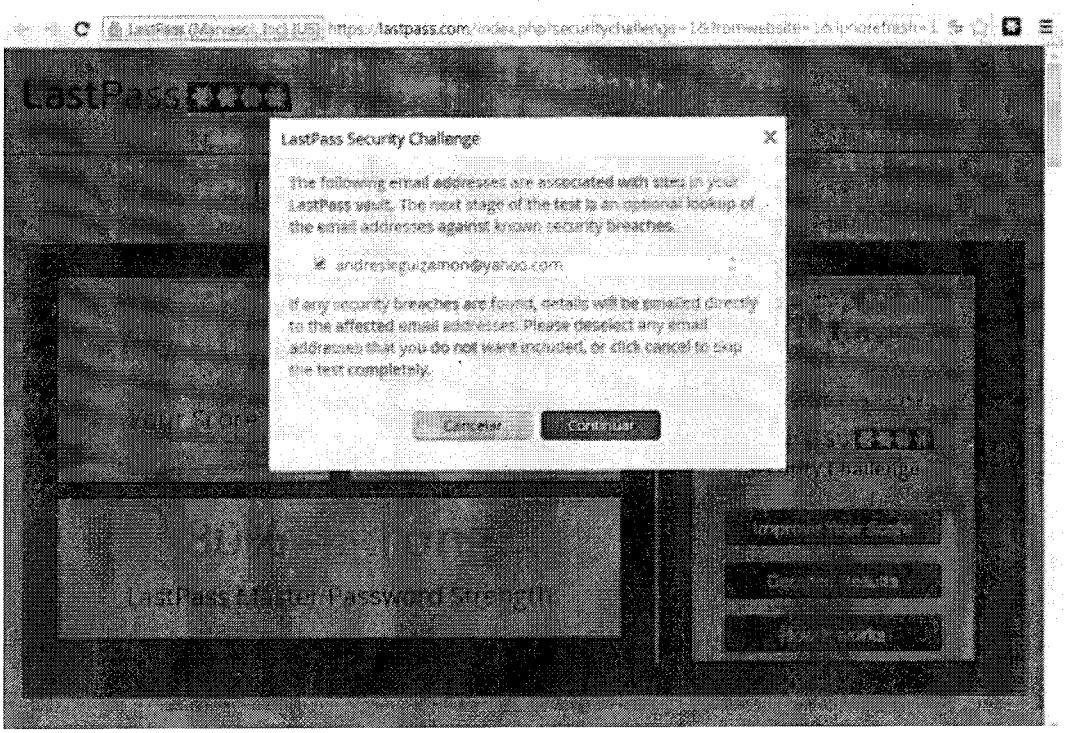


Ilustración 79 Información de certificado *LastPass*

8. *LastPass* hace una evaluación de la información subida por el usuario y a partir de esto muestra una calificación del nivel que tiene el usuario administrando sus datos con el objetivo de mostrar que tan segura es la forma en que el usuario guarda sus datos, denominado Desafio de

Seguridad *LastPass*:



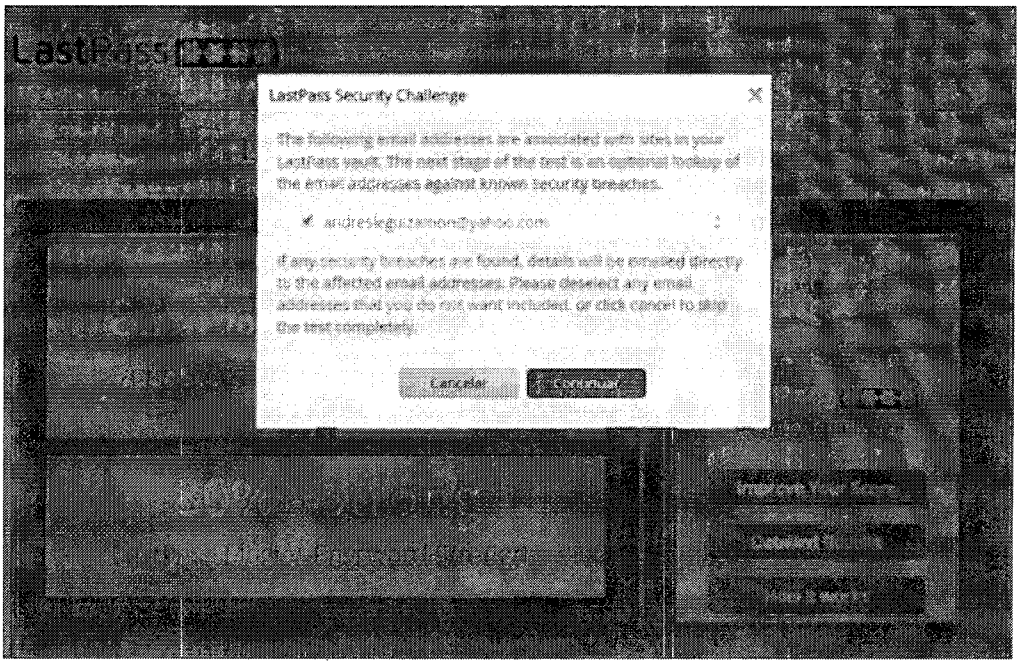


Ilustración 80 Desafío de seguridad *LastPass*

Forma de almacenamiento *LastPass*

1. Se accede a una página que solicita usuario y contraseña, en este caso Yahoo para el acceso a la cuenta de usuario.
2. El navegador muestra el mensaje de sugerencia "Autocompletado de contraseñas" para almacenar la contraseña.

Ilustración 81 Ingreso datos de usuario en *LastPass*

3. Posteriormente sale la ventana de *LastPass* donde se va a recordar el acceso a dicha cuenta:

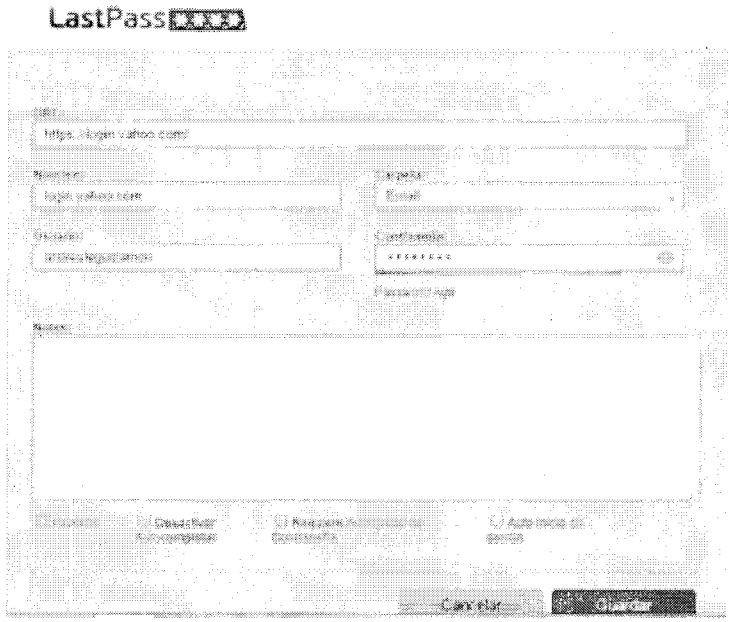


Ilustración 82 Edición de entradas en *LastPass*

4. En adelante, si se ha iniciado sesión con *LastPass*, se obtendrán los campos autocompletados de los servicios que se hayan guardado en la herramienta

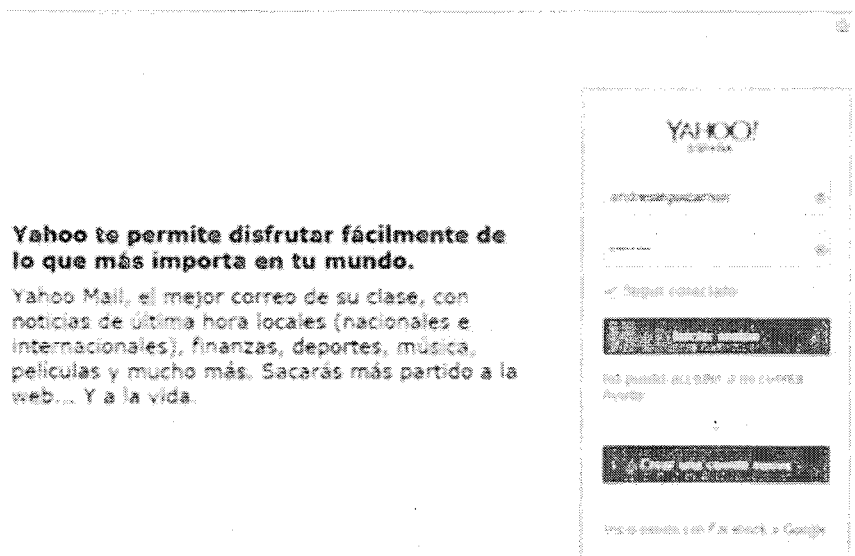


Ilustración 83 Autocompletado cada vez que se ingresa a la página web con datos ya ingresados *LastPass*

5. El almacén de las contraseñas y demás datos de usuario es como se ve a continuación:

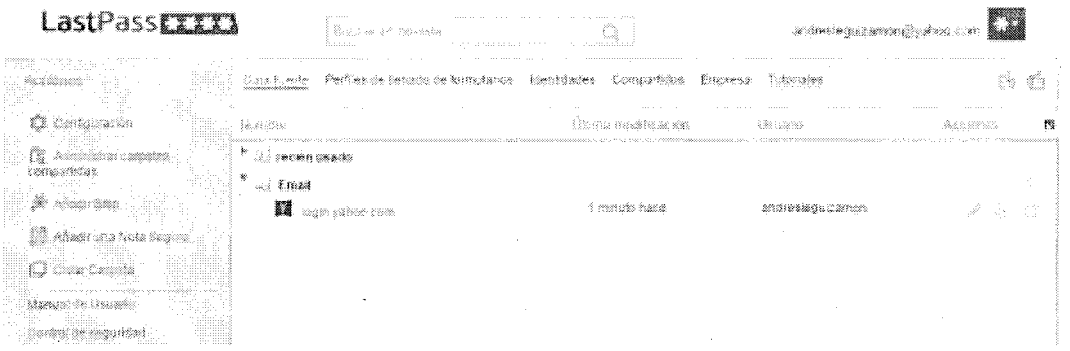


Ilustración 84 Almacén de datos *LastPass*

6. Las opciones para autocompletar los formularios de *LastPass* se ajustan según la necesidad. Cuando se entra a una página que tiene una cantidad de campos adicionales a la de un usuario y contraseña, se procede a guardar la página y los datos de una forma distinta: Se accede a la opción de herramientas y luego a guardar todos los campos. En esta ventana se procederá a guardar campo por campo según corresponda en la página especificada.

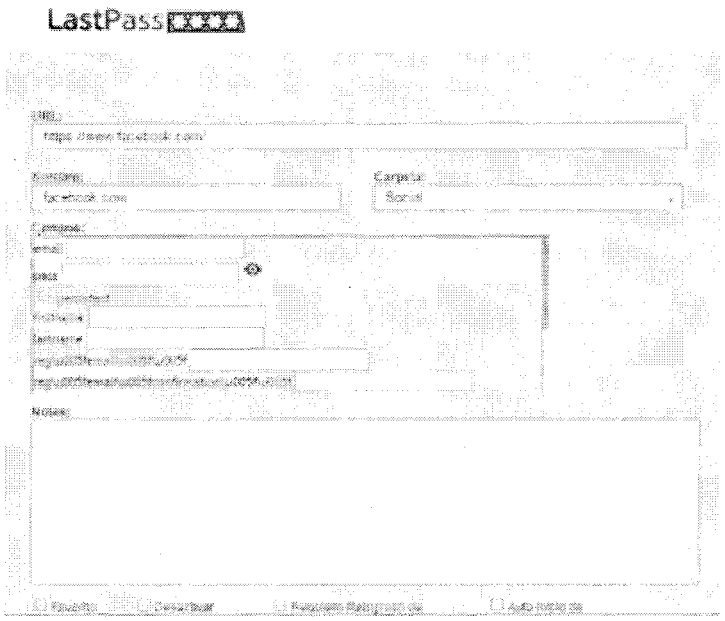


Ilustración 85 Configuración de entradas con campos adicionales *LastPass*

7. Para añadir el perfil en los formularios se accede a la opción correspondiente en el almacén de datos. Posteriormente se puede configurar el perfil y completar información personal, información de contacto, información de tarjeta de crédito, del banco y demás que completen el perfil de un usuario.

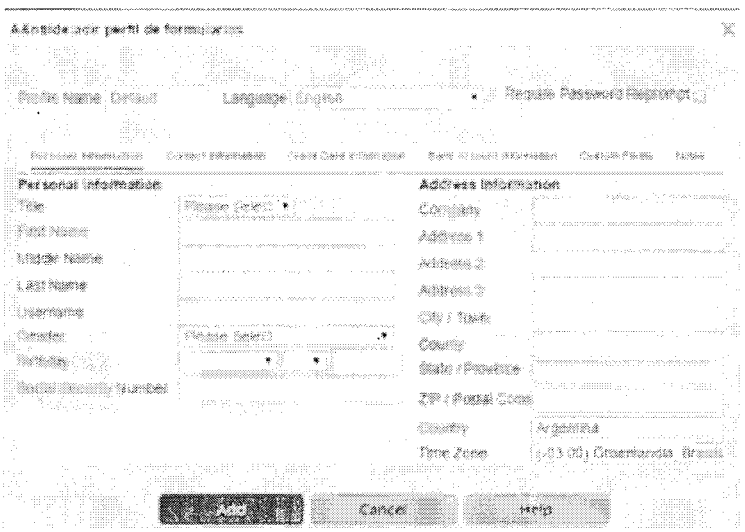


Ilustración 86 Edición formularios en *LastPass*

8. Se puede segmentar la vista separando identidades por ejemplo de temas escolares, de negocio y demás.

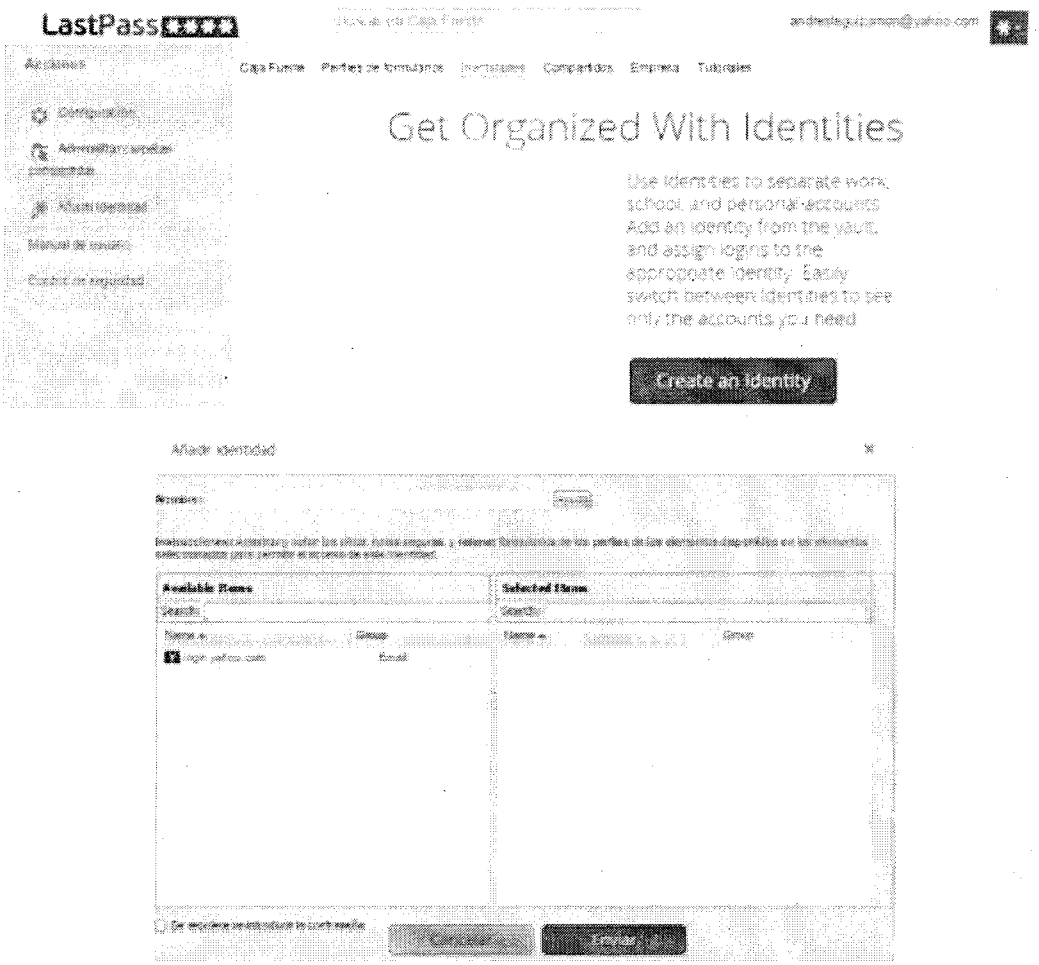


Ilustración 87 Organización de entradas por tipo de identidades en *LastPass*

9. Adicionalmente se pueden configurar cuentas compartidas:

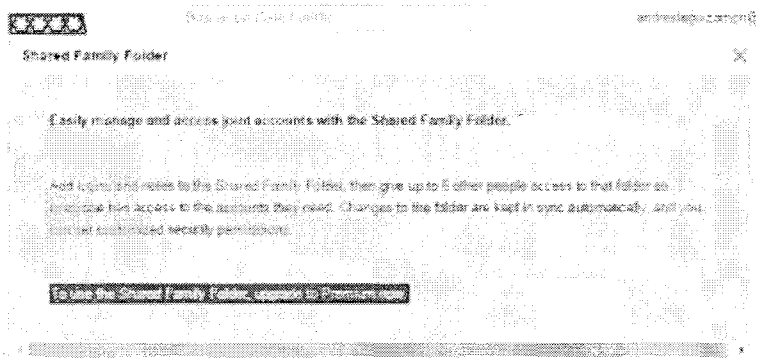


Ilustración 88 Configuración cuentas compartidas *LastPass*

Nota: *LastPass* es la única herramienta del estudio que implementa el uso de OTP, contraseña de un solo uso.

Ilustración 89 Uso de OTP en *LastPass*

10. Existe un módulo que permite ver la trazabilidad de los cambios que ha hecho el usuario sobre la herramienta.

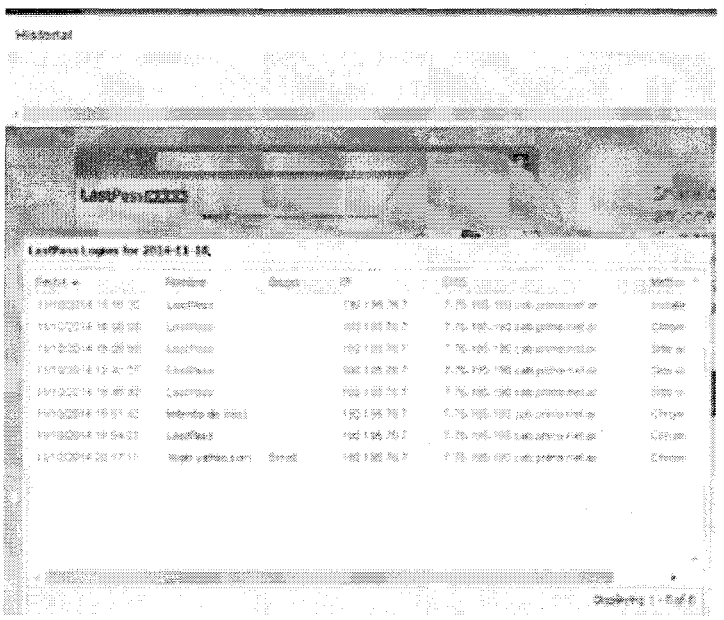


Ilustración 90 Trazabilidad de cambios en *LastPass*

El procedimiento para su configuración se describe a continuación [29]:

1. En primera instancia, se accede a la aplicación correspondiente y se selecciona la unidad en la cual va a ser instalado el software:

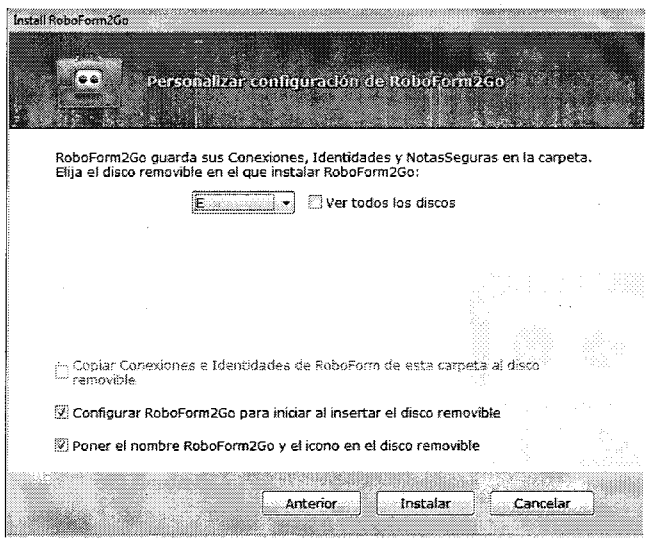


Ilustración 91 Instalación de *ROBOFORM* en dispositivo extraíble

2. Se elige el tipo de instalación, en este caso *Roboform2Go* debido a que la funcionalidad de *ROBOFORM* everywhere no está disponible en modo gratuito.

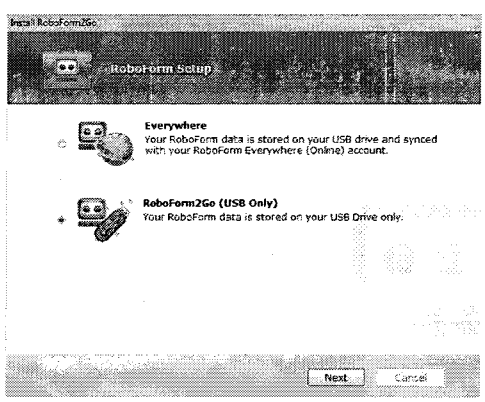


Ilustración 92 Instalación de *Roboform2Go* en dispositivo extraíble

3. Se introduce la *MASTER PASSWORD* del usuario. Es de gran utilidad la herramienta que viene automáticamente para generar contraseñas fuertes:

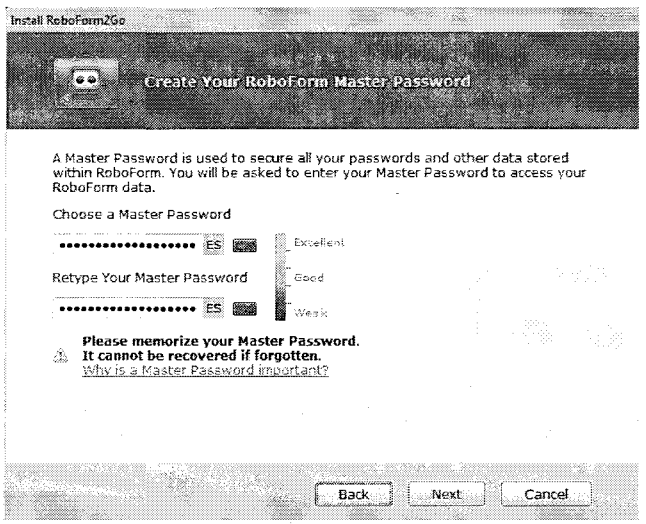


Ilustración 93 Creación del *MASTER PASSWORD*

4. El directorio de archivos queda como se ve a continuación en el dispositivo extraíble: la carpeta contiene los datos de usuarios y contraseñas. En el archivo *.RFT está el usuario y en el archivo *RFP está la contraseña. Si se requiere hacer un backup de los datos, hay que copiar todos los archivos del directorio. Si se requiere restaurar a una versión anterior de datos, hay que reemplazar los archivos anteriormente copiados en el directorio y reiniciar el software.

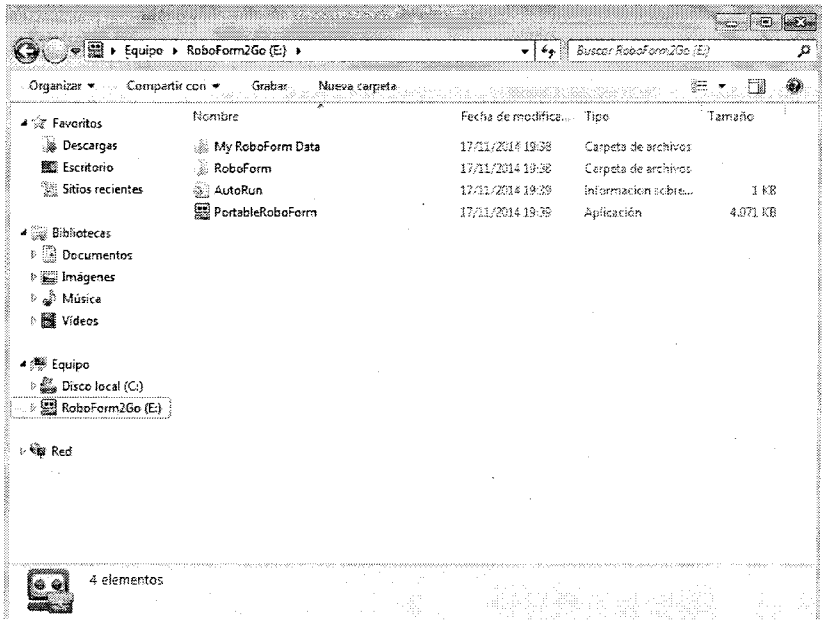


Ilustración 94 Directorio de archivos en dispositivo extraíble de *Roboform2Go*

5. A continuación se lanza el software desde el memoria *USB*:

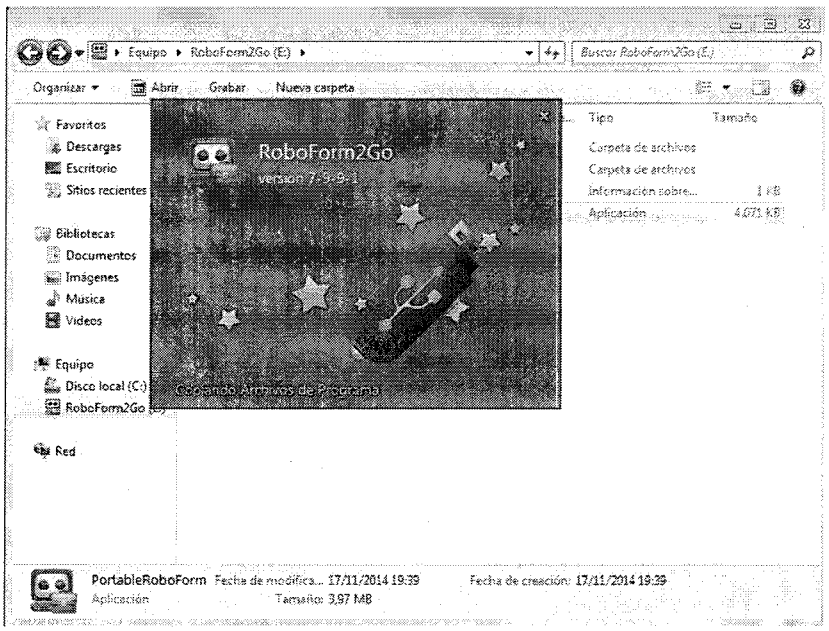


Ilustración 95 Ejecutar *Roboform2Go* desde dispositivo extraíble

6. Aparece el icono de la aplicación en la esquina inferior derecho:

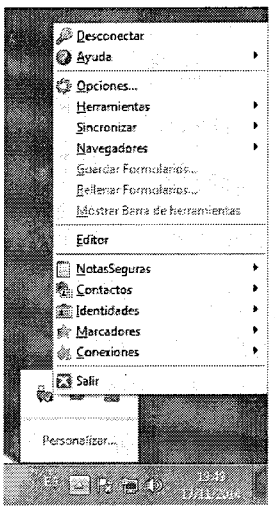


Ilustración 96 Menú de despliegue en *Windows* al conectar dispositivo con *Roboform2Go*

7. Se configura el idioma en las opciones de configuración de *ROBOFORM2GO*:

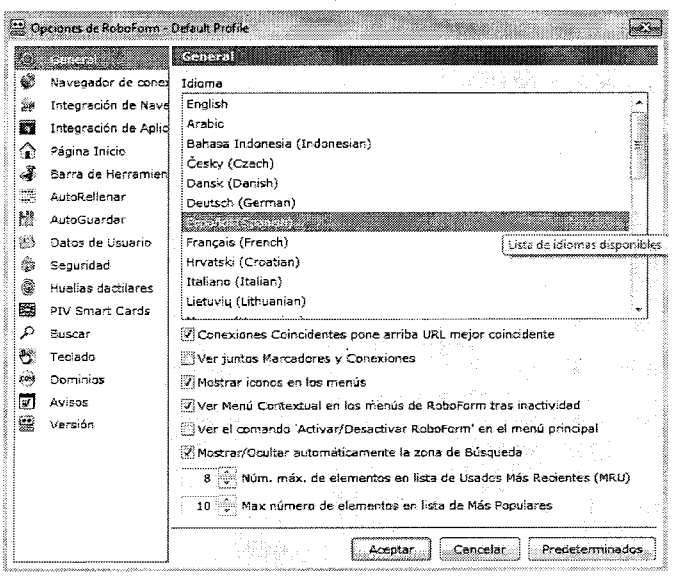


Ilustración 97 Configuración idioma *Roboform2Go*

8. Se puede elegir el navegador al cual estará acoplado *Roboform2Go* con el fin de que cuando aparezca un formulario para introducir contraseña y usuario, exista una barra en el navegador para gestionar los datos de usuario, a través de las opciones de Navegador de Conexión e Integración de Navegador:

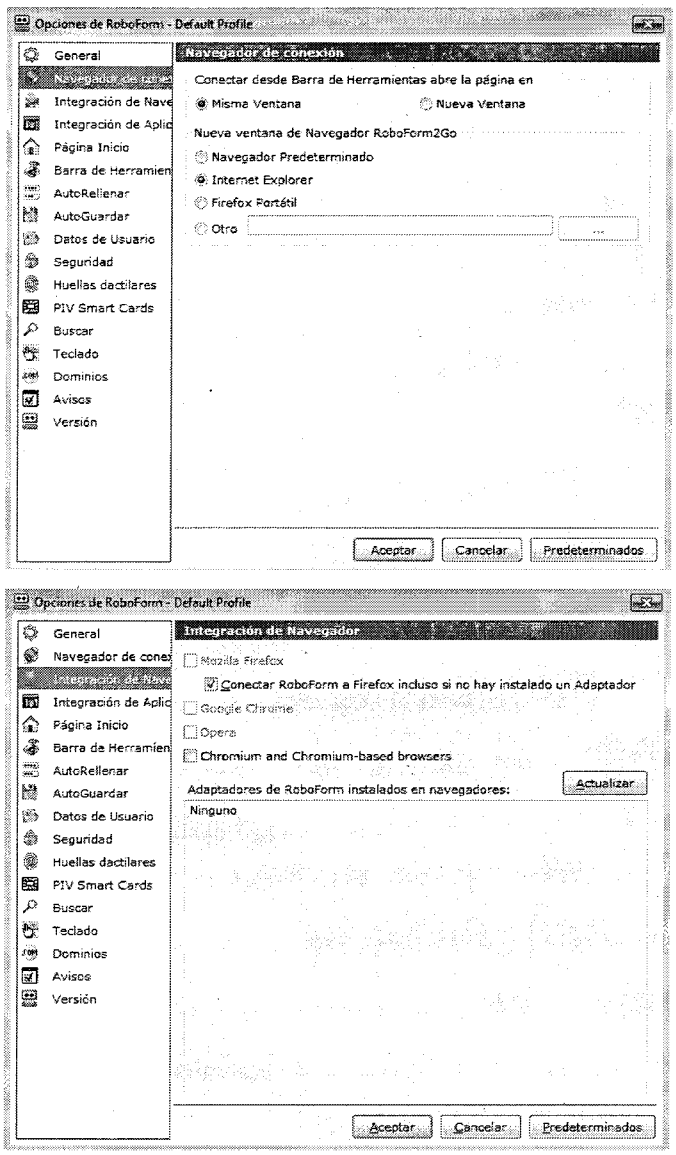


Ilustración 98 Configuración de navegador con *Roboform2Go*

9. A través de la opción de Integración de Aplicación se pueden gestionar aplicaciones de *Windows* que tengan uso de contraseña e id de usuario:

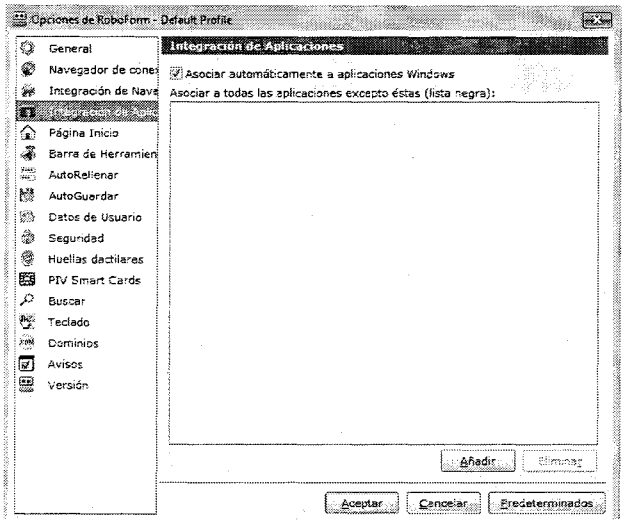
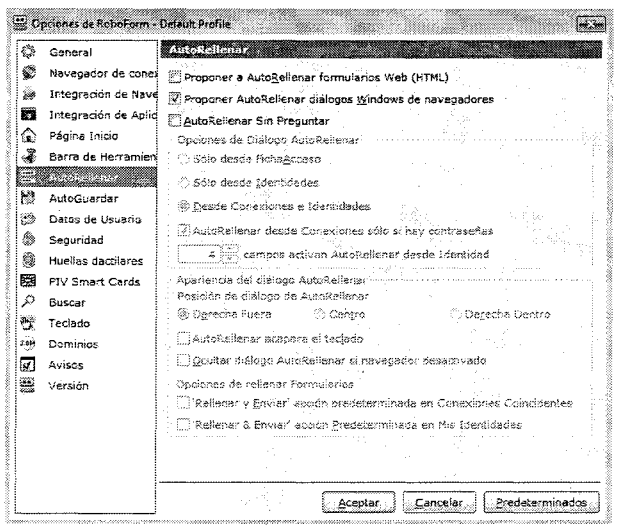


Ilustración 99 Integrar aplicaciones con *Roboform2Go*

10. Las opciones de autorellenar y autoguardar sirven para configurar la forma de completar y guardar la información de los formularios:



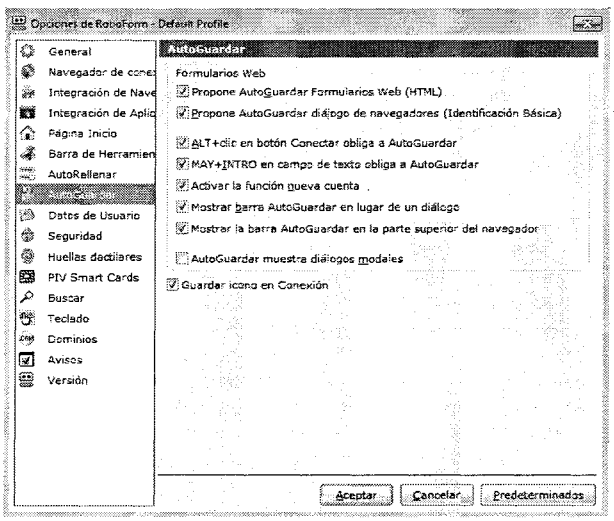


Ilustración 100 Autorellenar y autoguardar en *Roboform2Go*

11. En la sección de Seguridad se elige el algoritmo con el que se cifrará, a que se le va a poner contraseña (conexión, identidad, nota), la protección de memoria para borrar las contraseñas al desconectar el memoria *USB*, entre otras opciones:

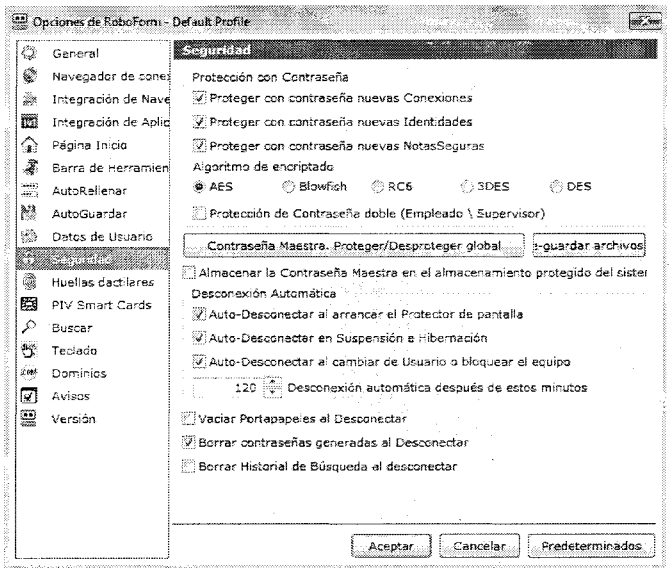


Ilustración 101 Configuración Seguridad *Roboform2Go*

12. Se puede configurar uso de biometría para conectar un lector de huellas digitales a *Roboform2Go*, en este caso no se configura este aspecto porque no se utiliza ningún lector biométrico de este tipo:

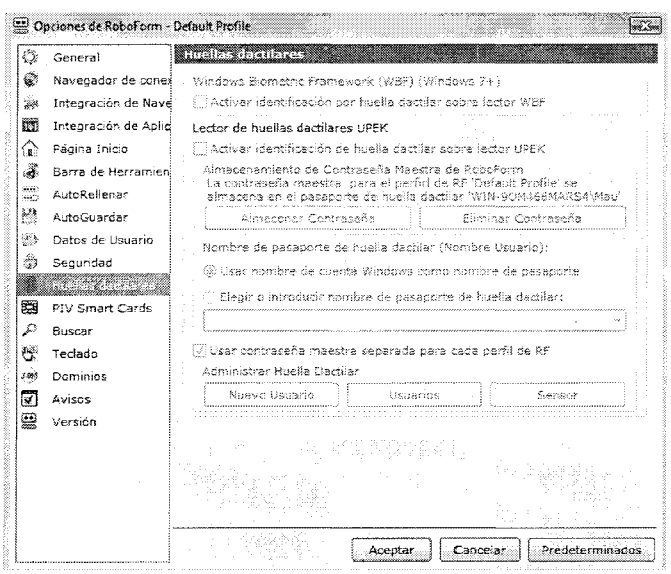


Ilustración 102 Uso de biometría *Roboform2Go*

13. Adicionalmente como factor de doble autenticación se puede conectar con tarjetas inteligentes PIV:

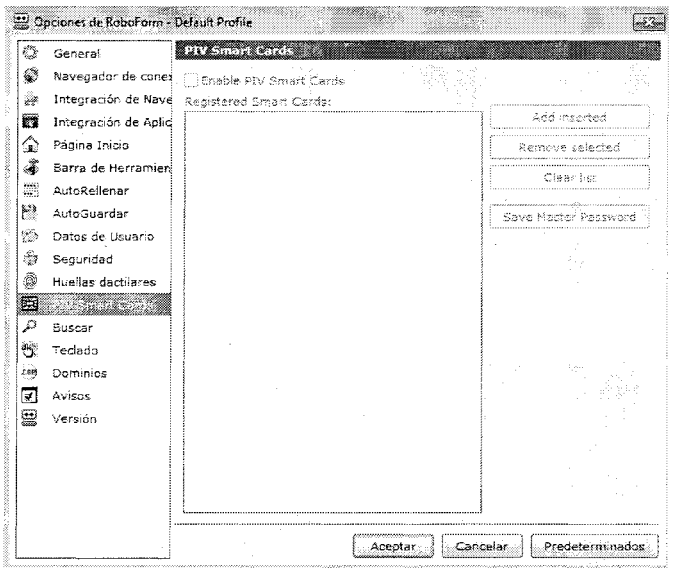


Ilustración 103 Uso de tarjetas PIV *Roboform2Go*

Forma de almacenamiento *Roboform2Go*

1. Para almacenar los datos en *Roboform2Go*, basta con haber lanzado la aplicación desde el memoria *USB*, a partir de esto se carga automáticamente en el navegador predeterminado que se haya prestablecido y a partir de esto se generara una barra de extensión en el navegador para que cuando se ingrese a una página, aparezca automáticamente la opción de autoguardar.

Ilustración 104 Guardar datos desde navegador en *Roboform2Go*

2. La barra aparece únicamente cuando se ejecuta el *Roboform2Go* desde la memoria *USB* asociado al navegador que se tiene por defecto.

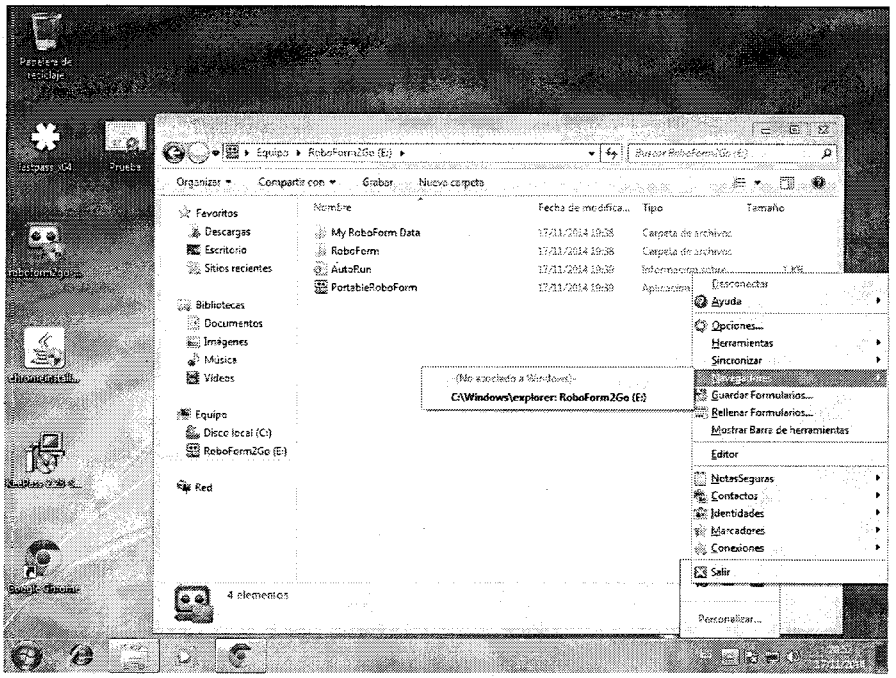


Ilustración 105 Asociación de navegador correspondiente con *Roboform2Go*

3. Cuando se guardan los datos, se puede acceder al almacén de datos para visualizarlos:

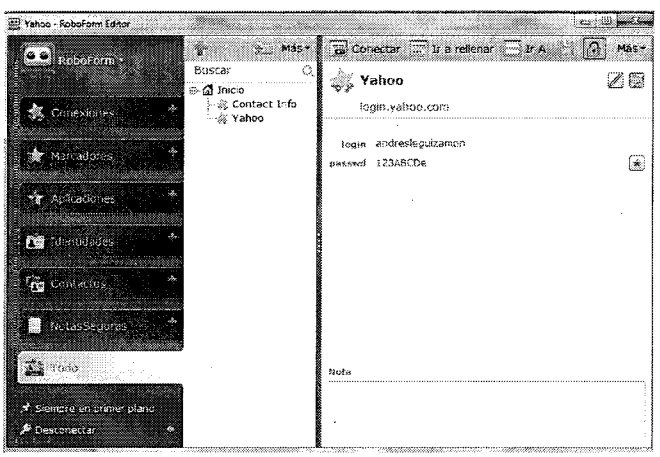


Ilustración 106 Acceso a almacén de datos *Roboform2Go*

VIII. Bibliografía

En orden de aparición en el texto:

[1] GOOGLE, GMAIL Y LA AUTENTICACIÓN DE DOBLE FACTOR (SMS CODE) http://www.seguridadparatodos.es/2011/11/google-gmail-y-la-autenticacion-de.html (consultada el 06/07/2014)

[2] Red Hat Enterprise *Linux* 4: Introducción a la administración de sistemas http://web.mit.edu/rhel-doc/4/RH-DOCS/rhel-isa-es-4/ch-acctsgrps.html (consultada el 08//08/2014)

[3] Consumer Password Worst Practices, IMPERVA, http://www.imperva.com/docs/wp_consumer_password_worst_practices.pdf (consultada el 25/07/2013)

[4] Administración efectiva de contraseñas https://seguridadetica.wordpress.com/2012/06/12/administacion-efectiva-de-contrasenas/ (consultada 06/06/2013)

[5] Read Write Web: Bad Form: 61% Use Same Password for Everything http://readwrite.com/2008/01/17/majority_use_same_password#awesm=~ogvjxapqCi831e (consultada el 06/07/2013)

[6] Los peligros de reutilizar contraseñas http://www.idnoticias.com/2014/12/11/los-peligros-de-reutilizar-las-contrasenas (consultada el 13/12/2014)

[7] Gestión de contraseñas, INTECO, http://www.inteco.es/Seguridad/Observatorio/Articulos/Gestion_contrasenas, (consultada el 25/07/2013)

[8] Light Blue Touchpaper Security Research, Computer Laboratory, University of Cambridge: Browser storage of passwords: a risk or opportunity? http://www.lightbluetouchpaper.org/2006/04/18/browser-storage-of-passwords-a-risk-or-opportunity/ (consultada el 08/07/2013)

[9] 'Citadel' Trojan Touts Trouble-Ticket System http://krebsonsecurity.com/2012/01/citadel-trojan-touts-trouble-ticket-system/ (consultada el 06/10/2014)

[10] Notorious Trojan Now Targets Password Managers http://www.tomsguide.com/us/citadel-trojan-password-managers,news-19942.html (consultada el 06/11/2014)

[11] Notificación *LastPass* Seguridad https://blog.*LastPass*.com/es/2011/05/*LastPass*-security-notification.html/ (consultada el 06/10/2014)

[12] *LastPass* Vulnerability Left IE Passwords Exposed, Update Now http://securitywatch.PCmag.com/security/314821-*LastPass*-vulnerability-left-ie-passwords-exposed-update-now (consultada el 06/10/2014)

[13] *LastPass* y el descubrimiento del Bug *HEARTBLEED* https://blog.*LastPass*.com/es/2014/04/*LastPass*-and-*HEARTBLEED*-bug.html/ y https://blog.*LastPass*.com/es/2014/06/your-*LastPass* (consultadas el 08/08/2014)

[14] OpenSSL Security Advisory https://www.openssl.org/news/secadv_20140407.txt (consultada el 08/08/2014)

[15] Common Vulnerabilities and Exposures, The Standard for Information Security Vulnerability Names https://cve.mitre.org (consultada el 20/06/2015)

[16] A New Class of Weak Keys for Blowfish http://www.iacr.org/archive/fse2007/45930168/45930168.pdf (consultada el 06/10/2014)

[17] Password Iterations PBKDF2 https://helpdesk.*LastPass*.com/es/security-options/password-iterations-pbkdf2/ fecha de consulta Noviembre 2014

[18] Definición Autenticación http://es.wikipedia.org/wiki/Autenticaci%C3%B3n (consultada el 22/12/2014)

[19] Glosario ISO 27000 http://www.iso27000.es/glosario.html (consultada el 13/06/2013)

[20] GNU General Public License https://es.wikipedia.org/wiki/GNU_General_Public_License (Consultada 30/06/2015)

[21] Definicion Hotkey http://www.digitalika.com/2012/05/hotkey-definicion-de-hoy/ (consultada el 22/12/2014)

[22] Definicion KEYLOGGER http://es.wikipedia.org/wiki/KEYLOGGER (consultada el 22/12/2014)

[23] Defining Malware: FAQ https://technet.microsoft.com/en-us/library/dd632948.aspx (consultada el 22/12/2014)

[24] Máquina Virtual http://www.itnews.ec/marco/000174.aspxz (consultada el 01/05/2013)

[25] ¿Qué es una frase de contraseña? http://*Windows*.microsoft.com/es-ar/*Windows*-vista/what-is-a-PASSPHRASE (consultada el 03/03/2014)

[26] Seguridad en Internet I. Características de los sistemas seguros y sistemas fiables. Tipos de amenazas generales. Amenazas a las comunicaciones.
http://documentacion.nexun.org/mediawiki/index.php/2 ._Seguridad_en_Internet_I._Caracter%C3%ADsticas_de_los_sistemas_seguros_y_sistemas_fiables._Tipos_de_amenazas_generales._Amenazas_a_las_comunicaciones.
(consultada el 01/05/2013)

[27] *KeePass*, http://*KeePass*.info/ (consultada el 06/07/2014)

[28] *LastPass*, https://*LastPass*.com/ (consultada el 06/07/2014)

[29] *Roboform2Go*: *ROBOFORM* on a *USB* Drive http://www.*ROBOFORM*.com/platforms/*Windows*/rf2go (consultada el 06/07/2014)

IX. Bibliografía General

En orden alfabético:

- Acissi, Seguridad Informática. Ethical Hacking. Conocer el ataque para una mejor defensa, Ediciones ENI, (2011), ISBN 2746068117, 9782746068117
- Arenburg Robert T., Chawla Sumit, Mathur Amit, Skawratananond Chakarat, Method, apparatus and program storage device for providing a secure password manager, United States Patent Application Publication, Chattanooga, 2007
- Brotzman Robert, Password Management Guideline, Department of Defense, Maryland, 1985
- Chiasson Sonia, Van Oorschot P.C., Biddle Robert, A Usability Study and Critique of Two Password Managers, School of Computer Science, Carleton University, Ottawa, 2006
- Cole Eric, Network Security Bible, John Wiley & Sons, (2011), ISBN 0470570008, 9780470570005
- Dei, H. Daniel, La tesis: Como orientarse en su elaboración, Buenos Aires, 2011
- Gibson Darril, Microsoft *Windows* Security Essentials, John Wiley & Sons, (2011), ISBN 111811454X, 9781118114544
- Phillips Bill, The Complete Book of Home, Site, and Office Security: Selecting, Installing, and Troubleshooting Systems and Devices, McGraw-Hill Proffessional, (2006), ISBN 0071467440, 9780071467445
- Roebuck Kevin, Password Management: High impact Strategies Emereo Pty Limited, 2011 ISBN 1743045018, 9781743045015
- Safriel Matnn, Portable password manager, United States Patent Application Publication, New York, 2004

Tablas

Ilustraciones