Seguridad y Acceso a la Información mediante una adecuada Gestión de Contraseñas

Edgardo José Castillo Rivera, ULACIT

13/04/2011

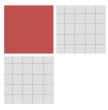


Tabla de contenido

Resumen

El proyecto investigativo sirve como respuesta a una necesidad creciente en el mayor porcentaje de usuarios de servicios de internet, así como en aplicaciones de sistemas locales, sobre: ¿Cómo asegurar el acceso a la información mediante una gestión adecuada de contraseñas?. Para ello, se ha realizado una investigación contemplando los malos hábitos en el uso de claves por parte de los usuarios. También, se han considerado los métodos que utilizan los atacantes para descubrir las contraseñas de un usuario y el objetivo que estas acciones conllevan.

De acuerdo al procedimiento de la investigación esta es principalmente cualitativa. Adicional, se ha tomado una muestra que está conformada por un universo de 60 personas con diversidad de nacionalidades, edades y grados académicos de América Latina. Debido a las limitaciones de la presente investigación se puede establecer que la porción representativa de la población seleccionada es una muestra por conveniencia.

A partir de los resultados obtenidos, se puede observar que se siguen evidenciando malas prácticas por parte de las personas en la creación y administración de contraseñas, lo que conlleva a un importante riesgo de seguridad. Es de suma importancia considerar que estas malas prácticas pueden estarse dando debido a que, la mayoría de los encuestados no tienen conocimientos sobre cómo trabajan los métodos disponibles para el manejo de contraseñas. Ya que la mayoría de los navegadores de Internet actuales, permiten

hacer uso de un gestor de contraseñas incorporado, de los cuales muchas personas hacen uso, pero sin entender aun la finalidad de seguridad y de protección que estos brindan a su información.

Abstract

This research project serves as a response to a growing need in the highest percentage of internet service users and local systems applications on: How to secure the access to information through the proper management of passwords?. To this end, research has been conducted looking at the bad habits in the use of keys by users. Also, we have considered the methods used by hackers to discover the password of a user and the objective that these actions entail.

According to this procedure the research is primarily qualitative. Further, it has taken a sample that consists of a universe of 60 people with a diversity of nationalities, ages and degrees of Latin America. Due to the limitations of this research may provide that a representative portion of the target population is a convenience sample.

From these results, we can see that continue to show wrongdoing by people in creating and managing passwords, leading to a major security risk. It is of utmost importance to consider these bad practices may be happening because the majority of respondents have no knowledge of how to work the methods available for managing passwords. Since most current Internet browsers allow use of a password manager built, of which many people use, but even without understanding the purpose of security and protection that they provide to their information.

Introducción

Las contraseñas son el primer nivel de seguridad establecido históricamente en el mundo de la informática. En cuanto se introdujo el concepto de multiusuario en las primeras máquinas UNIX, se hizo necesario proteger el acceso de alguna forma. Un usuario que comparte una computadora, no debía poder tener acceso a los mismos recursos que otro usuario y mucho menos el mismo nivel de control que el administrador. Lo más sencillo en aquel momento era establecer una contraseña que fuese conocida exclusivamente por el usuario para garantizar que solo él tuviese acceso a los recursos que le pertenecían. (INTECO, 2010)

Posteriormente con el auge que alcanzaron las redes, fueron surgiendo nuevos protocolos que permiten acceder a recursos ubicados físicamente en otra computadora. Para lo cual, fue necesaria una nueva metodología para restringir este tipo de acceso, tanto de la red como de los protocolos y aplicaciones. Sin embargo, a pesar de la creación de métodos más sofisticados de seguridad tales como *tokens* y biometría, siempre la utilización de contraseñas ha sido la forma preferente para proteger el acceso a diferentes recursos.

En los últimos años, el perfil de los usuarios de Internet y los usos que estos hacen de la Red, ha variado, alcanzándose unas notables tasas de penetración en determinados servicios. Así, por ejemplo en Latinoamérica, el correo electrónico, con un 85,5%, es el servicio más utilizado entre los usuarios habituales de Internet, seguido por las visitas a redes sociales con un 52,1%, un 34,2% ha utilizado servicios de banca electrónica y actividades financieras y el 33,5% ha

realizado compras online. El resultado de todo este proceso de incorporación a la sociedad de la información es que el número de dispositivos desde los que se puede acceder a las redes de información se ha ampliado y las gestiones desde los mismos son más numerosas, más frecuentes y de mayor trascendencia económica. (Jiménez, 2009)

Con el objetivo de que todo el proceso de comunicación sea de forma segura, cuando se hace uso de dichos servicios, se deben tomar ciertas medidas y buenas prácticas encaminadas a la mejora de la seguridad. Usualmente, cuando una persona hace uso de un servicio con una empresa a través de Internet, se le solicita una clave de usuario (*login*) y una contraseña (*password*). De esta manera, la concientización del usuario para gestionar de manera eficiente su información tiene uno de sus pilares en la correcta gestión y creación de las contraseñas que este ha de utilizar en la mayoría de los procesos y operaciones que requieran de su autenticación. (INTECO, 2007)

Diversos informes indican que es práctica habitual utilizar una misma contraseña para diferentes portales o servicios. Esto supone un peligro ya que, ante un potencial problema de seguridad en alguno de ellos que expusiese la contraseña a un atacante, sería sencillo tener acceso a otros recursos de la víctima utilizando la misma clave. Por lo que, observando los datos estadísticos sobre usos y hábitos en Internet, se constatan carencias y lagunas en la gestión de la seguridad de la información en relación con el empleo de las contraseñas. (The Imperva Application Defense Center (ADC), 2010)

La necesidad de hacer uso de diversos servicios, conlleva a la utilización de diferentes contraseñas como una buena práctica de seguridad. Sin embargo, la

tarea de gestión se incrementa para el usuario por lo que se hace necesario el uso de herramientas que ayuden a manejarlas de manera segura. Existen algunas soluciones de software que permiten una fácil administración, como Password Safe, Firefox's Password Manager y RoboForm, entre otros, que permiten a la vez su almacenamiento (y a veces, su creación) utilizando un cifrado fuerte de manera muy cómoda. Lo que proporciona una manera sencilla, cómoda y a la vez segura al usuario para el manejo de contraseñas.

Marco teórico

Mayor ataque de *phishing* de la historia

El 5 de octubre de 2009 se hizo público en una noticia, que los nombres de usuario y las contraseñas de más de 10.000 cuentas de correo electrónico de Hotmail habían sido hackeadas. El día posterior, según informó la BBC, se conoció que la lista se amplió a 30.000 cuentas e incluía servicios como Gmail, Yahoo y AOL (Fildes, 2009). Google confirmó que su servicio de correo electrónico se encontraba en el listado de las víctimas de *phishing* y al igual que hiciera Microsoft el día anterior, también anuncio medidas inmediatas para proteger a sus usuarios. (Keizer, 2009)

Consecuencias de la sustracción o revelación de las contraseñas

El objetivo de la sustracción de contraseñas, es para con ellas apropiarse de información sensible para el usuario con una finalidad de tipo económico o bien realizar otras acciones dañinas o delictivas como borrado de toda información, chantaje, espionaje industrial, etc. Las consecuencias son diversas y varían según el valor que cada usuario haya establecido para la información. (INTECO, 2007)

Si la contraseña corresponde a la de un servicio bancario podrían sustraer dinero de la cuenta o efectuar otras operaciones con perjuicio económico para el usuario. Si bien la contraseña pertenece a la computadora del hogar, se podría tomar su control o robar toda la información contenida en ella: como otras contraseñas o listados de usuarios y correos electrónicos o archivos personales y documentos.

Otra consecuencia podría ser el borrado completo de toda la información allí incluida.

En el ámbito laboral, las consecuencias pueden llegar a ser problemáticas si un tercero suplanta la identidad utilizando el usuario y su contraseña. Así, podría acceder a los sistemas corporativos con el usuario y de esta manera sustraer todo tipo de información del trabajador y/o la empresa o bien utilizar esta entrada para modificar o incluso eliminar archivos, con las consecuencias económicas, de responsabilidad jurídica y pérdidas de imagen que ello supondría.

Malos hábitos en el uso de contraseñas

La compañía Imperva realizó un estudio en el 2010 acerca de malas prácticas de las personas en la gestión de contraseñas. En el estudio se analizaron 32 millones de contraseñas reales de usuarios que habían sido obtenidas de un servicio Web y publicadas en diciembre del 2009. Las conclusiones más importantes extraídas del estudio fueron:

a) Aproximadamente un 50% de contraseñas constaba de siete caracteres o menos. Las contraseñas deben tener más de ocho caracteres. Para que estas sean de una longitud adecuada y además, sencillas de recordar, se pueden utilizar frases completas que pertenezcan a canciones, poemas o similares, que el usuario sea capaz de evocar fácilmente y que, aunque complejas, le resulten familiares. (INTECO, 2010)
b) El 40% sólo utilizaba letras en minúscula. Una contraseña robusta debe utilizar el mayor número posible de juegos de caracteres y mezclarlos. Esto

es, incluir letras mayúsculas, minúsculas, números y símbolos. Por ejemplo, se pueden usar los símbolos de interrogación, puntuación, etc., para crear una contraseña mucho más compleja. (INTECO, 2010)

Métodos por los que las contraseñas quedan al descubierto

Los métodos para descubrir las contraseñas de un usuario son variados. En primer lugar, se basan en la utilización de la ingeniería social (obtener información confidencial a través de la manipulación de usuarios legítimos), por ejemplo, utilizando el teléfono o un correo electrónico para engañar al usuario para que este revele sus contraseñas. Dentro de este grupo destaca el fraude conocido como *phishing* (delito encuadrado dentro del ámbito de las estafas cibernéticas). En este tipo de estafa online, el objetivo consiste en obtener las contraseñas o número de la tarjeta de un usuario, mediante un e-mail, sms, fax, etc. que suplanta la personalidad de una entidad de confianza y donde se le insta al usuario a que introduzca sus contraseñas de acceso. (Microsoft Corporation, 2011)

Es posible que el usuario se la comunique o ceda a un tercero y por accidente o descuido, quede expuesta al delincuente, por ejemplo, al teclearla delante de otras personas. Puede ser que el atacante conozca los hábitos del usuario y deduzca el sistema que este tiene para crear contraseñas (por ejemplo, que elige personajes de su libro favorito) o que asigne la misma contraseña a varios servicios (correo electrónico, código PIN de las tarjetas de crédito o teléfono móvil, contraseña de usuario en su computadora, etc.). En dado caso si se tiene la sospecha de que la contraseña pudo quedar expuesta, lo mejor es cambiarla antes de que se presente un inconveniente mayor. (Peredo, 2010)

Otro método, consiste en que el atacante pruebe contraseñas sucesivas hasta encontrar la que abre el sistema, lo que comúnmente se conoce por “ataque de fuerza bruta”. Actualmente un atacante con un equipo informático medio de los que hay en el mercado, podría probar hasta 10.000.000 de contraseñas por segundo. Esto significa que una clave creada con sólo letras minúsculas del alfabeto y con una longitud de seis caracteres, tardaría en ser descubierta aproximadamente en unos 30 segundos. Igualmente, se aplican técnicas más sofisticadas para realizar la intrusión. Se trata de métodos avanzados que consiguen averiguar la contraseña cifrada atacándola con un programa informático (“crackeador”) que la descodifica y deja al descubierto. (P., 2007)

Otro grupo de técnicas se basan en la previa infección del equipo mediante código malicioso: con programas “*sniffer*” o “*keylogger*”. Un programa “*sniffer*” o “monitor de red” espía las comunicaciones de la computadora que tiene residente dicho malware, a través de la red y de ellas obtiene los datos de las claves. El “keylogger” o “capturador de pulsaciones de teclado” consiste en un programa que se instala en la computadora del usuario de modo fraudulento y almacena en un archivo toda aquella información que se teclea en esta. Más adelante dicho archivo puede ser enviado al atacante sin conocimiento ni consentimiento del usuario y con ello, el intruso puede obtener las distintas contraseñas que el usuario ha utilizado en el acceso a los servicios online o que ha podido incluir en correos electrónicos. (INTECO, 2007)

Programas de gestión de contraseñas

Los programas de gestión de contraseñas ayudan a manejarlas de forma segura, sin necesidad de que se recuerden todas las que se necesitan. Además, permiten su almacenamiento (y a veces, su creación) utilizando un cifrado fuerte de manera muy cómoda. Esto facilita la administración de contraseñas y fomenta que los usuarios escojan claves complejas sin miedo a no ser capaces de recordarlas posteriormente. (INTECO, 2010)

Normalmente se basan en el cifrado fuerte de un archivo, que almacenará y ordenará todas las contraseñas. Para acceder al archivo cifrado, el usuario tendrá que recordar un único password, que suele ser llamado maestro o palabra de paso. Este permitirá el descifrado del archivo y por lo tanto, acceso al resto de las contraseñas almacenadas. Es de vital importancia, que esta palabra de paso sea muy robusta para que el resto no se vea en peligro. También es sumamente importante que no sea apuntada ni divulgada en forma alguna.

Usualmente, los programas para gestión de contraseñas brindan la opción de crear contraseñas automáticamente y de manera aleatoria, cumpliendo con buenas prácticas y a la vez facilitando la administración de las mismas para evitarle a los usuarios utilizar una misma clave para acceder a diferentes servicios. Además, esta clase de herramientas suelen incluir un medidor de robustez de contraseñas que le permite al usuario elegir sus propias claves al mismo tiempo que verifica su vulnerabilidad. Esta clase de programas suelen utilizar una clave de paso para acceder a la base de datos en la que se encuentran almacenadas todas las contraseñas que el usuario utiliza, por lo que se vuelve imprescindible

que esta sea lo menos vulnerable posible a ataques, para evitar que un tercero pueda tener acceso a las demás.

La mayoría de los navegadores de Internet actuales, como Safari, Firefox, Internet Explorer o Google Chrome, incorporan un complemento para gestionar contraseñas, al que adicionalmente se le puede restringir mediante una clave de paso. Esto facilita al usuario el tener que estar ingresando sus datos de autenticación cada vez que intenta acceder a un servicio determinado ya que, el navegador lo hace automáticamente, sin embargo, no es una operación aconsejable, ya que las contraseñas se almacenan en un servidor privado y puede suponer una pérdida en el control de las mismas. (Bonet, 2010)

Hacer uso de programas independientes de los navegadores como, LastPass o KeePass suele ser mejor, ya que es un método más seguro que almacenar las contraseñas en las páginas Web que brinden este tipo de servicios. A pesar de que este último método le permite al usuario portabilidad para accesar a sus claves desde cualquier sitio con conexión a Internet, la seguridad de las mismas dependerá del nivel de confianza que se dé a quien brinda el servicio. Adicional, los programas o complementos de gestión de contraseñas pueden ser utilizados como defensa contra el *phishing*, ya que la máquina puede distinguir entre dos páginas Web idénticas, pero con diferente dominio. Esto le garantiza al usuario que las claves no vayan a ser introducidas en una página no legítima.

Marco metodológico

Sampieri (2006), quien indica que “Un estudio no será mejor por tener una población más grande; la calidad de un trabajo investigativo estriba en delimitar claramente la población…” (p. 239).

La población de la presente investigación está conformada por un universo con diversidad de nacionalidades, edades y grados académicos de América Latina. Una vez delimitada la población, ha sido seleccionada una muestra no probabilística de 60 personas. El motivo de elección de este tipo de muestra se debe a las limitaciones humanas, geográficas, temporales, económicas, técnicas, y teóricas de este proyecto de investigación. Con los inconvenientes de la presente investigación se puede establecer que la porción representativa de la población seleccionada es una muestra por conveniencia.

Sampieri (2006) señala que “Las muestras por conveniencia son casos disponibles a los cuales tenemos acceso” (p. 571).

En el enfoque cualitativo, el diseño se refiere al abordaje general que se utiliza en el proceso de investigación. El cual proporciona a este estudio un marco metodológico que dará repuesta a la pregunta de investigación planteada. Este a su vez se caracteriza por la utilización del diseño cualitativo y cuantitativo en complementariedad. Pero se considera que de acuerdo al procedimiento de la investigación esta es principalmente cualitativa.

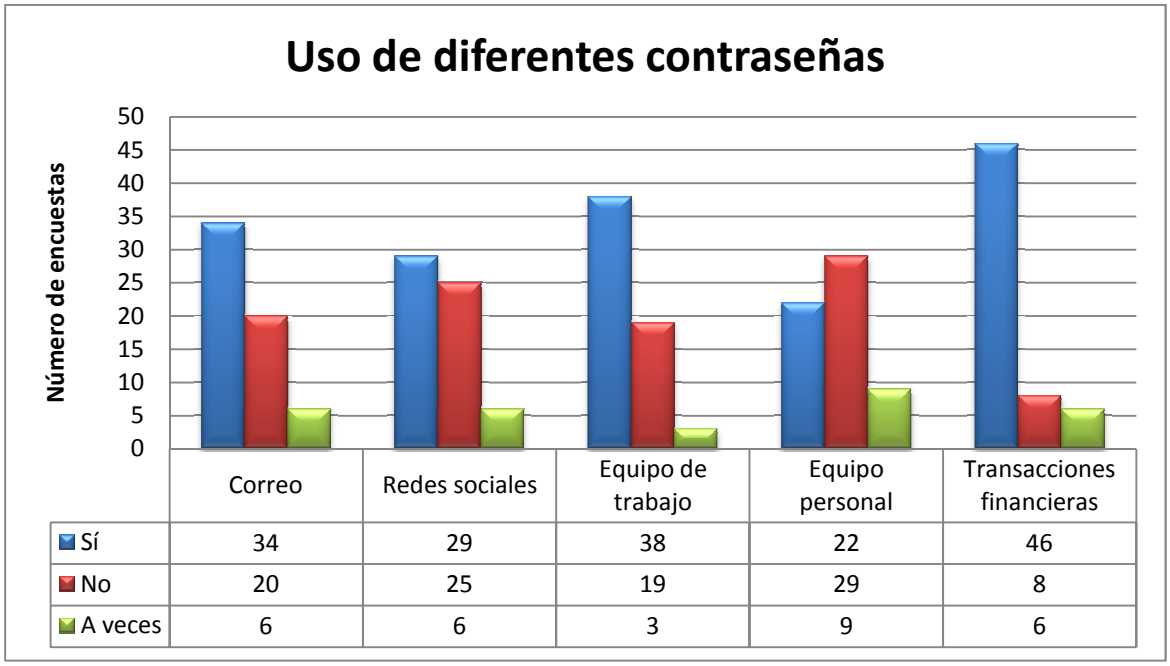
Se consideró en la aplicación de la encuesta, obtener los conocimientos generales de los encuestados sobre la creación y el posterior manejo que estos realizan de sus contraseñas. De esta manera se pueden clasificar los hábitos de las personas a la hora de hacer uso de diversos servicios en los que es necesaria la utilización de sus claves. Además, el propósito principal consiste en determinar la necesidad que la mayoría de las personas tienen de utilizar un método que les sirva para ayudarles a manejar eficazmente sus contraseñas a la vez que estos cumplen con recomendaciones de mejores prácticas para la creación y uso de las mismas. Sirve también, para conocer el porcentaje de personas que tienen conocimiento de este tipo de métodos, así como la cantidad que de estos, hace uso a la vez de los mismos.

La presente investigación puede considerarse confiable con un margen de error inferior a un 5%. Adicional de la muestra obtenida, los encuestados son de diversas nacionalidades de América Latina, estos se encuentran en un rango de edades y grado académico muy variado, pero todos con la característica común de hacer un uso constante de contraseñas para acceder a distintos tipos de servicios. Además, es importante considerar que debido a las limitaciones del proyecto, el muestreo realizado fue por conveniencia, por lo que no se garantiza que cada uno de los elementos de la población tuviese la misma oportunidad de ser tomado en cuenta. También debe considerarse que la aplicación de la encuesta no fue de manera personal, por lo que el margen de error de los resultados se limita a la sinceridad de las respuestas por parte de los encuestados.

Resultados de encuestas

GRÁFICO #1

Utilización de diferentes contraseñas para distintos fines



	Correo	Redes sociales	Equipo de trabajo	Equipo personal	Transacciones financieras
Sí	34	29	38	22	46
No	20	25	19	29	8
A veces	6	6	3	9	6

Se puede apreciar en el gráfico #1, que existen diferencias notables entre la manera de gestionar los diferentes tipos de cuentas que manejan los encuestados. Un 57% de los encuestados hace uso de diversas contraseñas para administrar sus cuentas de correos, mientras que un 10% lo hace a veces y el 33% restante no utiliza diferentes contraseñas para el manejo de sus correos. En cuanto a redes sociales un 48% utiliza diferentes contraseñas, mientras que un 10% lo hace regularmente y un 42% no cambia su contraseña en este tipo de servicios. En el uso de equipo de trabajo, un 63% hace uso de distintas contraseñas para hacer uso de las computadoras, solamente un 5% no lo hace siempre de esta manera, mientras que un considerable 32% no maneja distintas contraseñas para este fin.

Para el manejo de equipo personal, un 37% emplea distintas contraseñas para acceder a sus computadoras, mientras que un 15% hace cambios a veces y la mayoría con un 48% no cambia sus contraseñas para acceder a sus equipos. La mayoría de los encuestados, un 77% maneja diferentes contraseñas para realizar transacciones financieras, un 10% lo hace a veces y un 13% no cambia su contraseña para estos propósitos.

TABLA #1

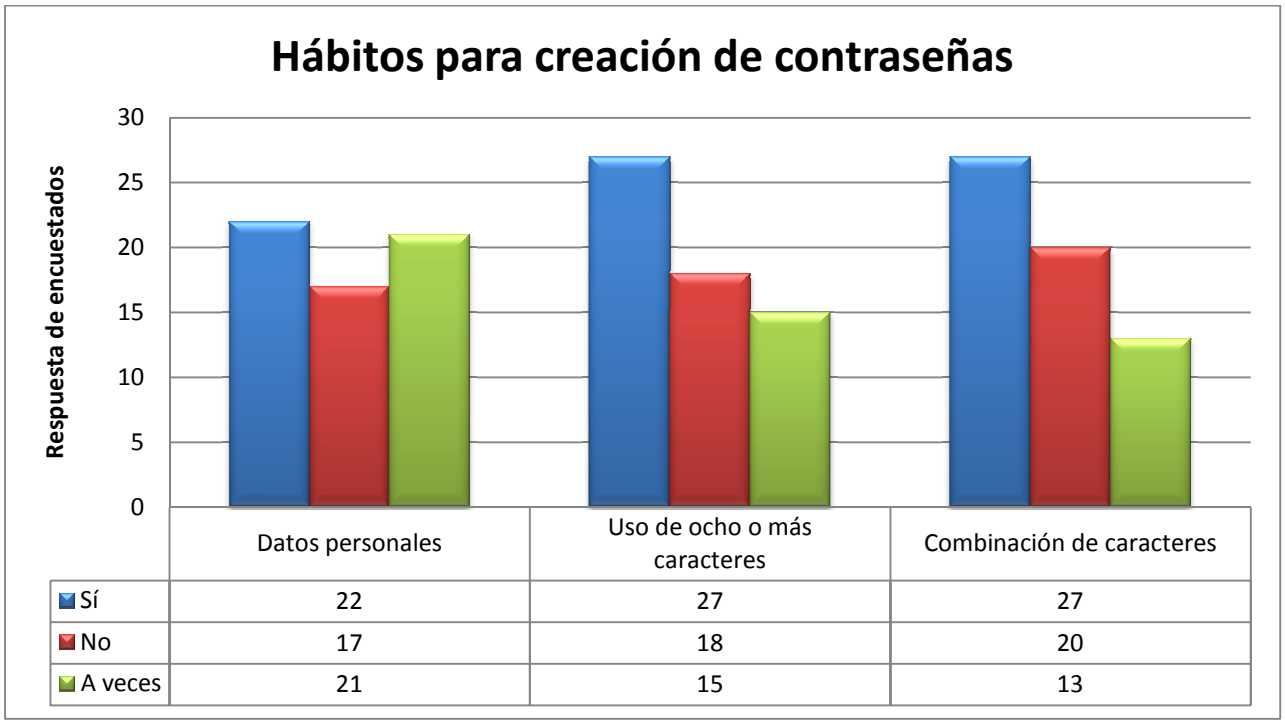
Cantidad de contraseñas manejadas

Cantidad de contraseñas usadas	Total	Porcentaje
1 a 5	21	35%
6 a 15	28	47%
16 o más	11	18%
Total	**60**	**100%**

La tabla #1 representa la cantidad de contraseñas más frecuentemente manejadas por los encuestados, de estos un 35% hace uso de una a cinco claves para distintos fines, un 46% maneja entre seis y quince distintas para realizar este cometido, mientras que un 18% requiere al menos de dieciséis de estas para hacer uso de diversos recursos.

GRÁFICO #2

Metodología utilizada para creación de contraseñas



De acuerdo con los resultados encontrados, en el gráfico #2 se manifiesta, que el 37% de los encuestados emplea datos personales en la creación de sus contraseñas, mientras que un 28% no lo hace y un 35% introduce a veces información personal en la elaboración de estas. Un 45% utiliza ocho o más caracteres en su creación, un 30% no utiliza al menos ocho caracteres, mientras que un 25% lo hace a veces.

TABLA #2

Cambios de contraseñas regulares

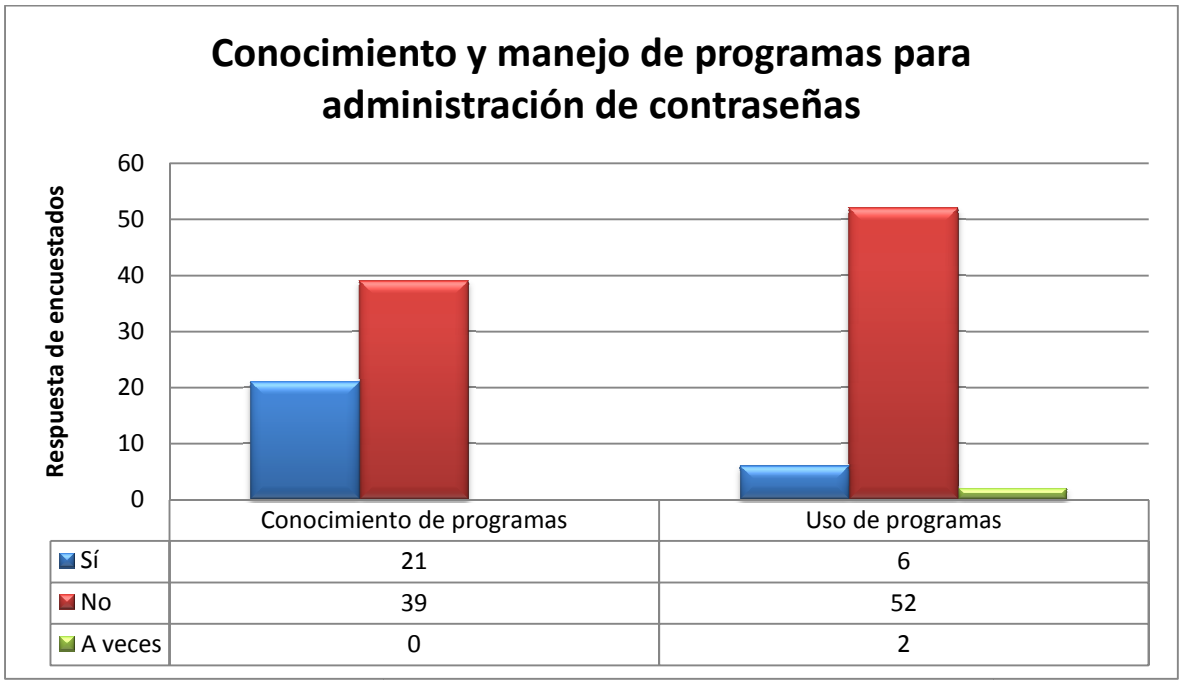
Cambios periódicos de contraseñas	Total	Porcentaje
Entre 1-7 días	2	3%
Entre 8-15 días	2	3%
Una vez al mes	4	7%
Cada tres meses	9	15%
Cada seis meses	10	17%
Una vez al año	17	28%
Nunca	16	27%
Total	**60**	**100%**

En la tabla #2, los resultados muestran que:

Un 27% de los encuestados no cambia sus contraseñas, el 28% lo hace una vez al año, mientras que el 17% lo hace cada seis meses y solamente el 28% lo hace en intervalos más cortos.

GRÁFICO #3

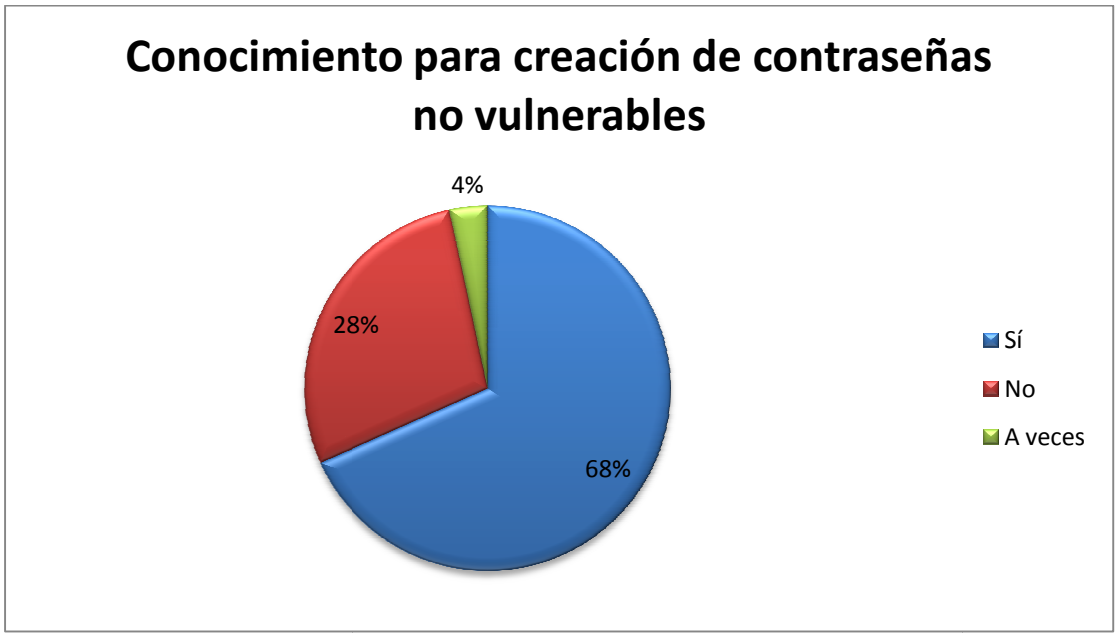
Conocimiento y uso de programas para administración de contraseñas



Mediante el análisis de los resultados que se muestran en el gráfico #3, se puede observar que un 35% tiene conocimientos acerca de programas para manejar contraseñas, mientras que el 65% no. Mas sin embargo, solo el 10% hace uso de esta clase de programas, un 3% los utiliza a veces y el 87% no.

GRÁFICO #4

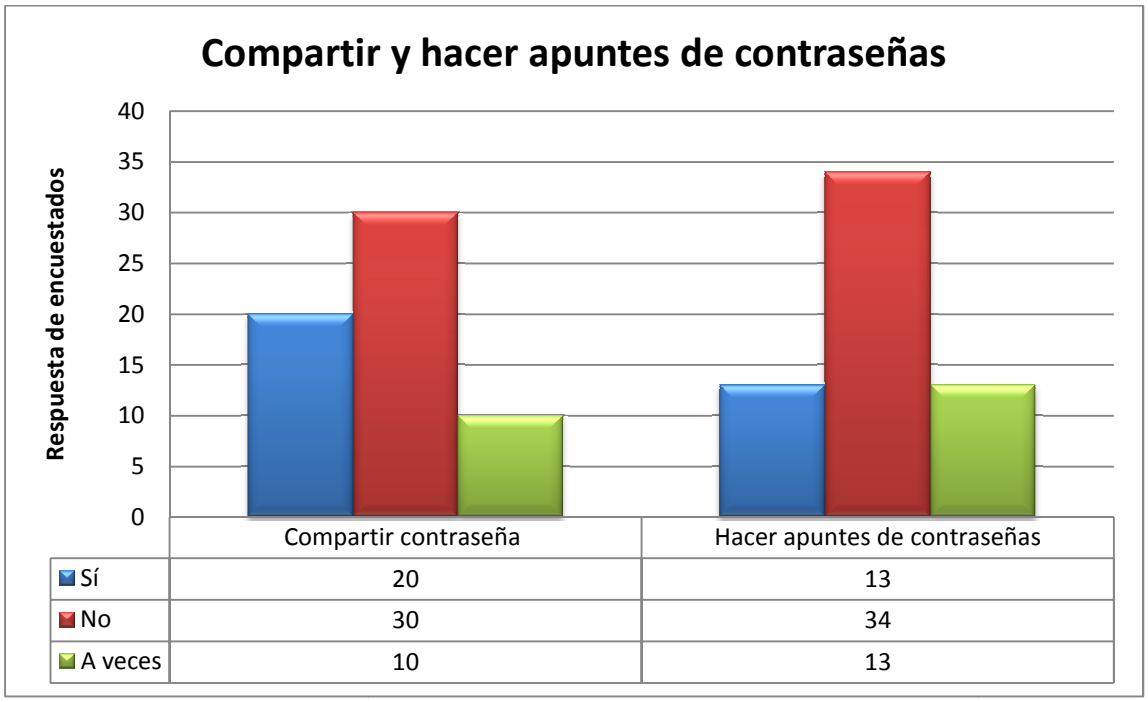
Conocimiento para creación de contraseñas no vulnerables a ataques



En el gráfico # 4 se puede apreciar que el 68% de los encuestados dice saber cómo crear una contraseña que no sea vulnerable, mientras que el 28% desconoce cómo hacerlo y un 4% tiene un poco de conocimiento al respecto.

GRÁFICO #5

Compartir contraseñas y hacer apuntes de ellas



	Compartir contraseña	Hacer apuntes de contraseñas
Sí	20	13
No	30	34
A veces	10	13

El gráfico # 5 muestra una práctica de los encuestados con respecto a compartir contraseñas con personas de confianza y a hacer apuntes de las mismas. Se estima que un 33% de los encuestados las comparten con alguien de confianza, mientras que el 50% no y un 17% lo hace a veces. Por otra parte, el 22% hace apuntes de sus contraseñas, mientras que un 56% no y un 22% lo hace regularmente.

TABLA #3

Identificación contraseña segura

Reconocimiento de contraseña segura	Total	Porcentaje
password1	3	5%
passw0rd2	2	3%
P@ssw0rd	23	38%
Passw0rd	20	33%
Ninguna	12	20%
Total	**60**	**100%**

En la tabla #3 se puede apreciar la percepción de los encuestados para identificar una contraseña segura.

El 39% de los encuestados identificó de manera correcta una contraseña que cumple con los requisitos mínimos para no ser vulnerable a ataques, mientras que el 41% reconoció otras claves que no satisfacen dichos requisitos y un 20% no supo identificar las que cumplen con los requerimientos mínimos.

GRÁFICO #6

Necesidad de método para administrar contraseñas

El gráfico #6 expresa los resultados obtenidos sobre la necesidad de un método para administración de contraseñas.

El 70% de los encuestados considera necesario un método para manejar sus contraseñas, mientras que el 18% no piensa que sea necesario y un 12% opina que a veces lo es.

Discusión

Es de suma importancia recalcar que las personas siguen incurriendo en diversos errores en cuanto a la utilización de contraseñas. Por ejemplo: en el gráfico #1 se puede notar que manejan un modelo para el uso de contraseñas acorde con la importancia del servicio que están utilizando, ya que la mayoría de los entrevistados hace uso de diversas contraseñas para transacciones financieras y para el equipo de trabajo, pero el número decrece para el uso de redes sociales y correo y lo hace aun más, para el uso de equipo personal. Por lo tanto, no dan importancia al hecho de que si alguien consigue acceso a alguno de los servicios que estos utilizan con menor precaución, podría fácilmente obtener diversa información personal, así como inclusive las contraseñas de los otros servicios que utiliza el usuario, ya que generalmente si se hace uso de claves robustas y a la vez se manejan más de seis en promedio, como se puede observar en la tabla #1, se suelen guardar como un respaldo por si se llegaran a olvidar.

Además, se puede observar en el gráfico #2, que a pesar de que la mayoría de las personas hacen uso de ocho o más caracteres en sus contraseñas y a la vez realizan una combinación de letras, números y símbolos, la mayoría también sigue haciendo uso de datos personales en estas, generalmente para hacerlas más fáciles de recordar. Adicionalmente como se observa en la tabla #2, únicamente el 28% de los encuestados cambia sus contraseñas en intervalos menores o iguales a tres meses. Por otro lado, en el gráfico #5 se nota que una cantidad importante de los encuestados siguen realizando algunas malas prácticas en el manejo de

contraseñas como ser, compartirlas con personas de confianza y hacer apuntes de estas.

Los anteriores resultados son patrones que se repiten una y otra vez en la mayoría de estudios sobre creación y gestión de contraseñas. Por lo tanto, estos resultados se pueden comparar con resultados de otros estudios como por ejemplo, “Como evitar las más Comunes y Peligrosas Contraseñas”. En dicho estudio, el 79% de usuarios utiliza malas prácticas para su creación, tanto desde usar menos de ocho caracteres como usar palabras que se puedan encontrar en el diccionario o claves que contengan información personal con pequeñas variaciones y no conlleven la combinación de símbolos, números y letras mayúsculas y minúsculas, las cuales son prácticas recomendables para que la contraseña no sea fácilmente vulnerable a ataques. (ZoneAlarm, 2011)

Por otra parte, es importante recalcar que la mayoría de los encuestados, el 68% (como se puede apreciar en el gráfico #4) considera que tiene los conocimientos necesarios para crear contraseñas que no sean vulnerables a ataques. A pesar de esto, solamente el 39%, como se puede observar en la tabla #3, pudo identificar correctamente cuál era la contraseña más segura de las opciones que se les presentaron. De esta manera queda en evidencia que el porcentaje de personas que no sabe cómo crear una contraseña segura, es considerablemente grande y a la vez, se sigue incurriendo en muchas malas prácticas en el manejo de estas.

Teniendo en cuenta que para poder acceder a la mayoría de servicios y recursos que se encuentran disponibles actualmente para las personas, tanto en Internet

como de manera local en las computadoras, se hace necesario el uso de contraseñas. Esto conlleva a que la mayoría de las personas como se puede apreciar en la tabla #1, haga uso al menos de seis y quince contraseñas, sumando a esto la necesidad de que las claves sean robustas y a la vez se estén cambiando en periodos cortos para poder asegurar el acceso a la información, se vuelve necesario el uso de un método para ayudarlas a manejar sus contraseñas, cumpliendo dichas consideraciones y a la vez facilitando la administración de las mismas. Esta necesidad se ve reflejada en el gráfico #6, ya que un 70% de los encuestados considera necesario un método para poder manejarlas.

El resultado de lo anterior es parte del proceso de incorporación a la sociedad de la información. El aumento notable en las tasas de penetración para acceder a las redes de datos, ha variado significativamente las gestiones y trascendencia que toman los usos que se hacen desde diversos dispositivos para determinados servicios. Estas gestiones son cada vez más numerosas y frecuentes, lo que a la vez ha incrementando considerablemente las tareas administrativas de identificación por parte de los usuarios, requiriendo de esta manera, una correcta gestión y creación de las contraseñas que se han de utilizar en las operaciones que requieren de su autenticación. (Jiménez, 2009)

A pesar de la creciente necesidad de un método para administrar contraseñas, se puede observar en el gráfico #3 que sin embargo, solamente el 10% de los encuestados hace uso de programas para el manejo de contraseñas. Además, se aprecia en este mismo, que el poco uso de programas para administrar contraseñas podría deberse a que el 65% de los encuestados no tienen

conocimiento acerca de estos programas y de los beneficios que podrían brindarles. Por otro lado, es importante recalcar que a pesar de que un 35% sí tiene conocimientos acerca de estos métodos para manejar contraseñas, solamente el 10% hace uso de los mismos, esto es una situación que debe ser considerada, ya que haciendo una comparación entre los porcentajes, únicamente el 28.6% del 100% que tiene conocimiento de esta clase de métodos, toma ventaja de los servicios que los mismos ofrecen.

Conclusiones

Se siguen evidenciando malas prácticas por parte de las personas en la creación y administración de contraseñas. Esto conlleva a un importante riesgo de seguridad para que terceros puedan obtener acceso a información personal que puede culminar con intrusiones en equipos con información más sensible como pueden ser los equipos de trabajo o inclusive robos de identidad. De esta manera, se debe considerar de forma prioritaria el uso de contraseñas que no sean vulnerables a ataques para todo tipo de servicio al que se tiene acceso.

Es importante recalcar que la mayoría de los encuestados no tienen conocimientos sobre métodos disponibles para el manejo de contraseñas. Esto conlleva muchas veces a la elaboración de pocas contraseñas que a estos se les hagan fáciles de recordar y con un nivel de complejidad no tan grande con el mismo fin. Se puede asumir que aun no existe suficiente concientización y conocimiento en las personas de la relevancia que están adquiriendo estas con las nuevas tendencias de tecnologías de computación en la nube, mismas que se están encargando día a día de que toda la información pase a estar totalmente en la red con diversos servicios a través de la plataforma de Internet. A pesar de los beneficios que responden a múltiples características integradas en esta tendencia, se aumentan los riesgos de que terceros accedan a la misma con gran facilidad, ya que se pierde de algún modo el control. De esta manera, se vuelve aun más indispensable realizar una adecuada gestión de contraseñas.

Cabe destacar que la mayoría de los navegadores de Internet actuales, permiten hacer uso de un gestor de contraseñas incorporado. Por lo que a pesar de que

así, muchas personas hacen uso de estos complementos, aun no han comprendido la finalidad de la seguridad y la protección que estos brindan a su información. También se vuelve más fácil la introducción de herramientas de gestión de contraseñas con la finalidad de proteger el acceso a información de carácter personal.

Considerando los aspectos anteriores, se vuelve necesario, la utilización de un método que permita al usuario cumplir con dichos fines de manera inmediata sin necesitar hacer uso de un mayor esfuerzo. Con este fin los programas para administración de contraseñas le permitirán al usuario, no solamente el manejo de una mayor cantidad de contraseñas, en vista de lo necesario que se vuelven día a día para más servicios, sino también hasta la creación de las mismas para que cumplan con las mejores prácticas para la creación de contraseñas. Además, muchos de los programas ofrecen movilidad, lo que permite poder utilizarlas en cualquier lugar, siempre teniendo únicamente precauciones sobre la confianza de dichos lugares.

Bibliografía

Libros

Sampieri, Collado, & Baptista. (2006). *Metodología de la Investigación* (Cuarta ed.). México: McGraw Hill Interamericana.

Medios electrónicos en Internet

Bonet, J. (15 de agosto de 2010). *Alternativa segura al gestor de contraseñas de tu navegador*. Recuperado el 12 de marzo de 2011, de http://lastpass.softonic.com/

Fildes, J. (6 de octubre de 2009). *Google targeted in e-mail scam* . Recuperado el 15 de marzo de 2011, de http://news.bbc.co.uk/2/hi/technology/8292928.stm

INTECO. (13 de setiembre de 2010). *Password Management*. Recuperado el 24 de febrero de 2011, de http://www.inteco.es/file/r3X8PRtuZbJ7bnjy14-vEQ

INTECO. (8 de noviembre de 2007). *Password policy and information security*. Recuperado el 22 de febrero de 2011, de

http://www.inteco.es/file/knfyV3nSImwq8a9E2V9T6g

Jiménez, C. (19 de noviembre de 2009). *Cómo usa Internet el latinoamericano*. Recuperado el 19 de 2 de 2011, de http://www.tendenciasdigitales.com/503/como-usa-internet-ellatinoamericano/

Keizer, G. (5 de octubre de 2009). *Microsoft confirms phishers stole 'several thousand' Hotmail passwords*. Recuperado el 15 de marzo de 2011, de http://www.computerworld.com/s/article/9138956/Microsoft_confirms_phishers_stole_several_thousand_Hotmail_passwords

Microsoft Corporation. (10 de enero de 2011). *Reconozca las estafas por suplantación de identidad (phishing) y los mensajes de correo electrónico fraudulentos*. Recuperado el 2 de marzo de 2011, de http://www.microsoft.com/latam/protect/yourself/phishing/identify.mspx

P., J. (26 de marzo de 2007). *How I'd Hack Your Weak Passwords*. Recuperado el 5 de marzo de 2011, de http://onemansblog.com/2007/03/26/how-id-hack-your-weak-passwords/

Peredo. (11 de marzo de 2010). *Importancia de contar con Passwords seguros*. Recuperado el 5 de marzo de 2011, de http://logit42.com/archives/1496

Pickard, A. (17 de enero de 2008). *Are you suffering from password pressure?* Recuperado el 19 de

febrero de 2011, de

http://www.guardian.co.uk/technology/2008/jan/17/security.banks

Schneier, B. (14 de diciembre de 2006). *MySpace Passwords Aren't So Dumb*. Recuperado el 28 de febrero de 2011, de

ttp://www.wired.com/politics/security/commentary/securitymatters/2006/12/72300

SEGURIDAD INTERNET. (10 de noviembre de 2008). *Contraseña*. Recuperado el 25 de febrero de 2011, de

http://miguel-seguridadinternet.blogspot.com/2008/11/contrasea.html

The Imperva Application Defense Center (ADC). (1 de abril de 2010). *Consumer Password Worst Practices*. Recuperado el 19 de febrero de 2011, de

http://www.imperva.com/docs/WP_Consumer_Password_Worst_Practices.pdf

The Telegraph. (2 de setiembre de 2009). *Security risk as people use same password on all websites*. Recuperado el 19 de febrero de 2011, de

http://www.telegraph.co.uk/technology/news/6125081/Security-risk-as-people-use-same-password-on-all-websites.html

ZoneAlarm. (12 de febrero de 2011). *How to Avoid the Most Common and Dangerous Passwords*. Recuperado el 20 de marzo de 2011, de

http://blog.zonealarm.com/2011/01/securing-yourself-from-a-world-of-hackers.html?view=infographic

Anexos

Instrumento de investigación

Estimado(a) encuestado(a):
El presente cuestionario forma parte de un estudio universitario que el estudiante Edgardo Castillo Rivera está realizando con el fin de conocer la necesidad de gestionar las contraseñas para una mayor seguridad y acceso a la información, para el curso de seminario de graduación. El cuestionario es fácil y rápido de completar y cuenta con 18 preguntas se estima que usted deberá disponer de unos 5 a 10 minutos para responderlo.
Su participación en este estudio es voluntaria y anónima. Los resultados serán de uso estrictamente interno de ULACIT en forma de cuadros y gráficos con datos totales y porcentuales. Se le solicita contestar de forma objetiva, pues el propósito es contar con un diagnóstico del tema y sus implicaciones para Latinoamérica. Si tiene alguna pregunta sobre la naturaleza y los objetivos de la encuesta, o sobre el cuestionario propiamente dicho, puede comunicarse con mi persona.

Instrucciones:
Leer con claridad los ítems, contestar de manera sincera, y seleccionar la opción con una “x”.

1. Utiliza diferentes contraseñas para:
   Correo(s) _____ Si _____ No _____ A veces
   Red(es) Social(es) _____ Si _____ No _____ A veces
   Equipo de trabajo _____ Si _____ No _____ A veces
   Equipo personal _____ Si _____ No _____ A veces
   Transacciones financieras _____ Si _____ No _____ A veces
2. Cuantas contraseñas maneja
   _____ 1-5
   _____ 10-15
   _____ 15 o más
3. Hace uso de datos personales en su(s) contraseña(s)
   _____ Si _____ No _____ A veces
4. Utiliza ocho o más caracteres en su(s) contraseña(s)
   _____ Si _____ No _____ A veces
5. Utiliza una combinación de letras, números y símbolos en su(s) contraseña(s)
   _____ Si _____ No _____ A veces
6. Cambia su(s) contraseña(s) regularmente
   _____ Entre 1-7 días
   _____ Entre 8-15 días
   _____ Una vez al mes
   _____ Cada tres meses
   _____ Cada seis meses

_____ Una vez al año
_____ Nunca

7. Hace uso de un comprobador de contraseñas, para ayudarle a medir la seguridad de su(s) contraseña(s)
   _____ Si _____ No _____ A veces
8. Tiene conocimiento de algún método existente para obtener la contraseña de una persona
   _____ Si _____ No _____ A veces
9. Hace uso de algún programa para la creación de su(s) contraseña()
   _____ Si _____ No _____ A veces
10. Tiene conocimiento de algún programa para administrar su(s) contraseña(s)
    _____ Si _____ No _____ A veces
11. Hace uso de algún programa para administración de contraseñas
    _____ Si _____ No _____ A veces
12. Sabe cómo crear una contraseña que no sea vulnerable a ataques
    _____ Si _____ No _____ A veces
13. Comparte su(s) contraseña(s) con alguien de confianza
    _____ Si _____ No _____ A veces
14. Hace apuntes de su(s) contraseña(s) en algún sitio
    _____ Si _____ No _____ A veces
15. Cuál de las siguientes contraseñas consideras segura
    _____ password1
    _____ passw0rd2
    _____ P@ssw0rd
    _____ Passw0rd
    _____ Ninguna
16. Considera necesario un método para administrar su(s) contraseña(s)
    _____ Si _____ No _____ A veces
17. En que rango de edad se encuentra
    _____ Menor de 18 años
    _____ Entre 19 y 25 años
    _____ Entre 26 y 35 años
    _____ Entre 36 y 45 años
    _____ Mayor de 45 años
18. Qué nivel de estudios posee
    _____ Secundaria
    _____ Bachillerato
    _____ Licenciatura
    _____ Maestría
    _____ Doctorado

¡Muchas gracias por su colaboración!