Universidad Nacional Autónoma de México

Programa de Posgrado en Ciencia de la Administración

T e s i s

Impacto de la Ingeniería Social en la Seguridad de la Información del Sector Financiero

Que para obtener el grado de:

Maestro en Administración

Campo de Conocimiento Administración de la Tecnología

Presenta: Anaid Guevara Soriano

Tutor (Director de la tesis): Mtro. Luis Fernando Zúñiga López

México, D.F. 2012

Dedicatoria

Dedico éste trabajo *primeramente a Dios* porque me ha dado la fortaleza, sabiduría e inteligencia para seguir avante en todos los caminos de mi vida tanto personal como profesional

A mi familia, como un testimonio de mi infinito aprecio y agradecimiento por toda una vida de esfuerzos y sacrificios, brindándome siempre cariño y apoyo cuando más lo necesité. Deseo de todo corazón que mi triunfo profesional lo sientan como suyo.

Pero sobre todo te dedico éste triunfo *a ti mami*, ya que maravillosa es la oportunidad para agradecer y reconocer el tesón que empeñaste sin reserva en pos de mi pleno desarrollo profesional. Mi gratitud inmensa por tus horas de desvelo, tu franco regaño y tu sabio consejo. Invaluable tesoro que aquilato y acojo. Por el enorme impulso que en todo momento me dio la fuerza y la voluntad en mi misión por ser alguien en la vida, por la fe sin límite que tuviste en mí, por tu grandeza infinita.

Agradecimiento

Por su invaluable apoyo, sabiduría y presencia en todo mi trayecto:

A mi mami

Por su apoyo incondicional en todo momento, su sabiduría y guía constante:

Mi tutor y sinodal *Mtro. Luis Fernando Zúñiga López*; mi sinodal y tutor metodológico *Dr. Carlos Eduardo Puga Murguía* y mi sinodal *Dr. José Alfredo Delgado Guzmán*

A mis sinodales por su confianza y apoyo:

Dr. Adrián Méndez Salvatorio

Mtro. Alfredo Corona Cabrera

A mis compañeros y amigos que estuvieron siempre presentes en mi vida profesional tanto de la carrera como de la maestría.

A mi alma mater la *Universidad Nacional Autónoma de México* por acogerme con cariño y permitirme obtener otro logro más en mi vida tanto profesional como personal.

Con amor, admiración y respeto

Ing. Anaid Guevara Soriano

ÍNDICE

INTRODUCCIÓN

Hoy en día es común saber de constantes ataques informáticos que atentan contra la seguridad de la información, sobre todo en el ámbito empresarial y organizacional y en muchos de los casos de vital importancia. Aunado a ello, el índice de fraudes electrónicos y fuga de información en las organizaciones que va en incremento, sobre todo en el sector financiero, ya que suele ser una fuente vitalicia para la extracción monetaria de manera fácil por parte de delincuentes cibernéticos como los crackers. No obstante, las entidades financieras han implementado medidas y controles tanto físicos como lógicos para reducir los índices de fraudes y robo. Sin embargo, estos van en aumento, razón por la cual representa un problema que requiere de constante atención.

Partiendo de esta problemática, surge la inquietud de realizar una investigación encaminada hacia la importancia de la seguridad de la información y a la amenaza latente de ataques informáticos a los que están expuestos todos los usuarios de equipo de cómputo y telecomunicaciones de forma consciente y en muchos casos inconsciente al ser abordados con técnicas que desconocen, como la ingeniería social, la cual puede tener un uso benéfico o malicioso según su aplicación, como es el caso del hacking que no necesariamente representa robo o fraude.

Derivado de lo anterior, el objetivo del presente trabajo es Identificar el impacto de la Ingeniería Social en la seguridad de la información de las instituciones de Banca Múltiple (BM) y de Banca de Desarrollo (BD) del sector financiero en el Distrito Federal, para con ello abonar en la concientización de los actores en las instituciones del riesgo constante que pueden tener al no invertir en la capacitación de sus empleados respecto a la importancia de la seguridad de la información y los tipos de ataques informáticos a los que están expuestos, inversión que puede beneficiar en la protección y reducción del índice de fuga de información, trayendo consigo múltiples beneficios entre ellos indudablemente el monetario.

El presente trabajo consta de cinco capítulos los cuales se describen a continuación:

El Primer Capítulo integra un marco de referencia respecto al tema del Hacking Ético o también llamado Ethical Hacking, en el cual se abordan los antecedentes del hacking ético, el cómo éste surgió, lo qué es, las vertientes que tiene, las diferencias entre los términos hacker y cracker, así como las secciones a analizar dentro de un auditoría de hacking ético según la metodología OSSTMM- Open Source Security Testing Methodology Manual.

Partiendo del Capítulo I, en el Capítulo II se aborda una de las secciones más importantes a evaluar durante una auditoría de hacking ético, me refiero a la Ingeniería Social, técnica de la que previamente se planteó su procedencia en la metodología OSSTMM y de la cual parte el punto medular de este trabajo de investigación. Dicho capítulo explica el significado de la Ingeniería Social, así como su importancia y los estudios realizados respecto a dicho tema.

En el Capítulo III se plantean aspectos relevantes dentro del sector financiero, tales como la cultura organizacional respecto a la seguridad informática con la que cuentan las organizaciones dentro del sector financiero, la importancia de la seguridad de la información en el sector financiero y los métodos de seguridad implementados en las organizaciones financieras para combatir los robos informáticos, así como los fraudes tanto físicos como electrónicos.

Subsecuentemente, el Capítulo IV refiere a la Metodología empleada en donde se expone el tipo de estudio empleado para dicha investigación, las etapas del diseño de investigación que se llevaron a cabo, la población considerada para la investigación, así como la unidad de análisis a la cual se aplicó el instrumento. Así mismo, se expone el diseño de muestreo en el cual se determinó el tamaño de la muestra, los criterios de inclusión y exclusión para la misma, la identificación, definición y operacionalización de las variables y los instrumentos que se emplearon para evaluar y analizar el estudio.

En lo que respecto al Capítulo V se exponen los resultados obtenidos una vez aplicado el instrumento en el estudio de campo correspondiente.

Finalmente, un apartado de conclusiones y recomendaciones pertinentes una vez finalizada la investigación, así mismo, se incluyen las referencias bibliográficas empleadas para el desarrollo de esta investigación. Además se concluye un apartado de anexos donde se ubica el instrumento empleado para la investigación, así como gráficos, instrumentos empleados por otras investigaciones acorde a la investigación, tablas, entre otros elementos cuya inclusión se consideró pertinente a lo largo del estudio.

PLANTEAMIENTO DEL PROBLEMA

En la actualidad, hemos sido testigos de las múltiples fugas de información que se presentan en empresas y organizaciones, primordialmente en el sector financiero, lo que conlleva a grandes pérdidas de índole material, así como monetarias. Dicho factor ha tenido presencia con mayor intensidad al paso del tiempo y las preguntas ante él son: ¿Por qué esta situación? ¿Qué es lo que genera dichas pérdidas? ¿Qué le hace falta a la organización para mermar las fugas de información? o ¿cuál es o cuáles son los puntos vulnerables por los cuales se da la fuga de la información?

En la búsqueda de una respuesta concreta que resuelva tales cuestiones surge el término de la ingeniería social, que se define, según especialistas en la materia y sitios underground del hacking, como una técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían. Precisamente, éste es el punto cúspide de la investigación, ya que al omitir esta técnica empleada común e innatamente en nuestra vida diaria por parte de los individuos, y primordialmente de aquellos llamados "crackers y hackers", estamos siendo cómplices y al mismo tiempo víctimas de la divulgación de información confidencial que puede ser utilizada con fines maliciosos y en contra de los objetivos y metas de las empresas; tal es el caso de las instituciones de Banca Múltiple y de Banca de Desarrollo mexicanas del Distrito Federal, dentro del sector financiero.

Es por ello que mi postura referente a este tan controvertido tema es el de que dicha fuga de información se da debido a la falta de cultura de seguridad de la información existente en las empresas y organizaciones, primordialmente abocándome a las entidades de índole financiero en el Distrito Federal, ya que es estrictamente aquí en donde "supuestamente" el nivel de seguridad en todos los ámbitos debe ser fuertemente estructurado; sin embargo, la seguridad de la información sigue en peligro debido a que no todos los integrantes del corporativo tiene dicha cultura ni tienen nociones con respecto al manejo del término de la ingeniería social. Si hubiese una difusión adecuada y extendida del peligro que acecha la divulgación de información confidencial y personal, tanto de la organización como del individuo a cualquier ente como lo son amigos, conocidos, extraños, etcétera, la divulgación de información inconsciente y por consiguiente las fugas de información confidencial de dichas instituciones disminuirían en gran escala y en consecuencia se evitarían las pérdidas financieras exacerbadas.

DELIMITACIÓN DEL PROBLEMA

Se abordó de manera general la problemática que se presenta respecto al hacking en las empresas, haciendo énfasis primordial en una de las técnicas comúnmente empleadas para la obtención de la información de una manera fácil y eficaz. Para ello se hace hincapié en la Ingeniería Social y el impacto que su aplicación tiene respecto a la seguridad de la información en las instituciones mexicanas de Banca Múltiple y de Banca de Desarrollo del Distrito Federal dentro del sector financiero; lo anterior, con la finalidad de detectar y evaluar el nivel de conocimiento respecto de la Ingeniería Social con el que cuentan los empleados de las instituciones antes mencionadas. Ya que si existe una carencia del mismo, la seguridad de la información de las instituciones de Banca Múltiple y de Banca de Desarrollo quedará expuesta y por ende éstas serán susceptibles de ataques informáticos suscitados con frecuencia, lo que traerá como consecuencia el que se atente contra la confidencialidad, integridad y disponibilidad de la información sensitiva de las instituciones correspondientes.

ESQUEMA DE ANÁLISIS DE VARIABLES

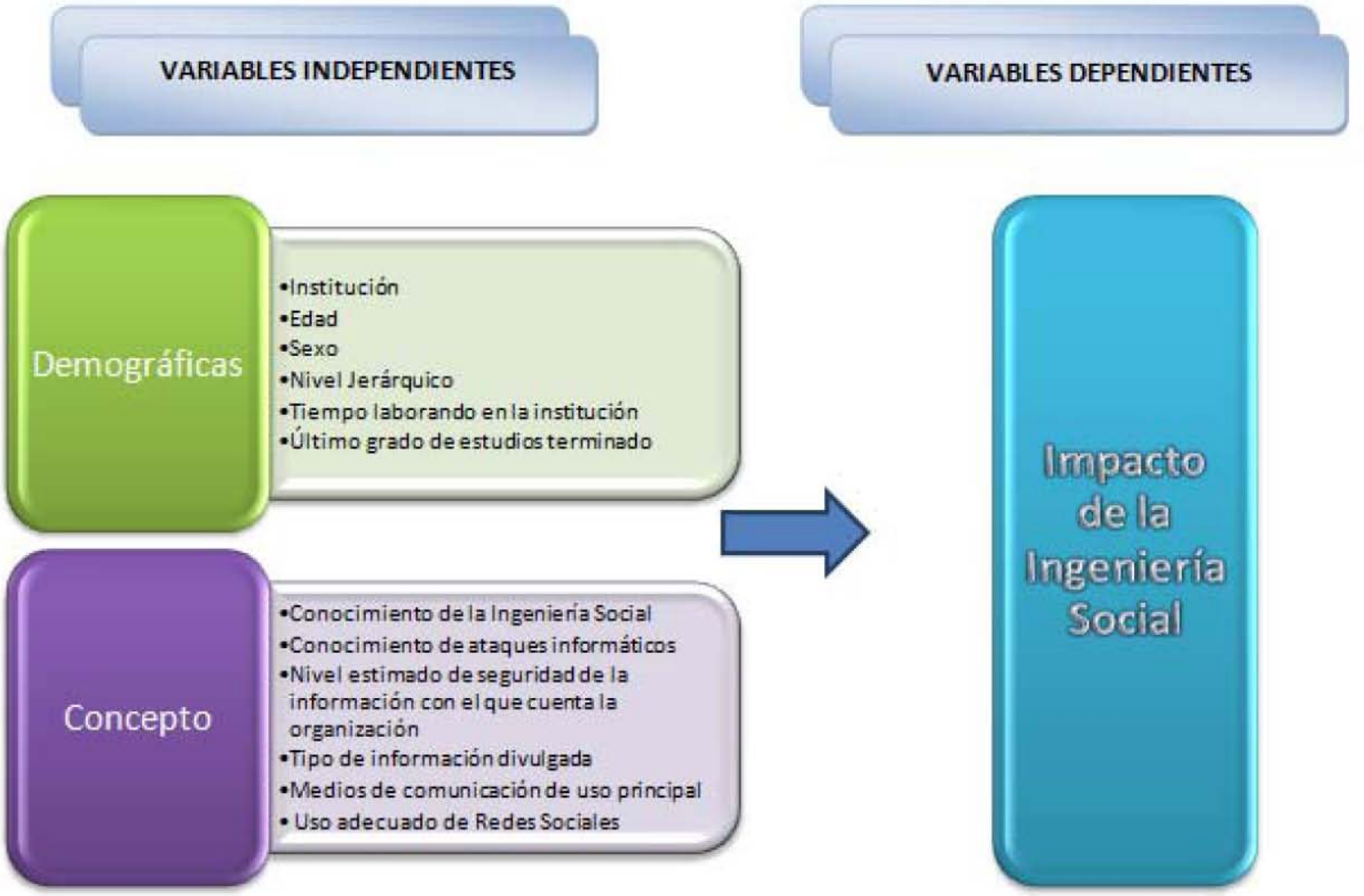


Fig. 1 Análisis de variables. Fuente: Elaboración propia del autor.

PREGUNTAS DE INVESTIGACIÓN

¿Cuál es el impacto de la Ingeniería Social en la seguridad de la información de las instituciones de Banca Múltiple (BM) y de Banca de Desarrollo (BD) del sector financiero en el Distrito Federal?

1. ¿Cuál es la relación de la Seguridad de la Información con el Hacking Ético y la Ingeniería Social?
2. ¿Es la Ingeniería Social un tema del conocimiento del personal que labora en las instituciones de BM y de BD del sector financiero en el Distrito Federal?
3. ¿Tendrán los empleados de las instituciones de BM y de BD del Distrito Federal conocimiento de los ataques informáticos a los que están expuestos al hacer uso de un equipo de cómputo y telecomunicaciones?
4. ¿Por qué medios comparten información los empleados de las instituciones de BM y de BD según su tipo?
5. ¿Influye la edad, nivel jerárquico y educativo en la cultura de la seguridad de la información?
6. ¿Es la Ingeniería Social un instrumento que puede contribuir a determinar la cultura de la seguridad de la información en instituciones de BM y de BD en el sector financiero?

OBJETIVOS

GENERAL

Identificar el impacto de la Ingeniería Social en la seguridad de la información de las instituciones de Banca Múltiple (BM) y de Banca de Desarrollo (BD) del sector financiero en el Distrito Federal.

ESPECÍFICOS

1. Hacer una recuperación documental acerca del papel del Hacking Ético en la Seguridad de la Información y su relación con la Ingeniería Social.
2. Identificar el conocimiento que tiene el personal que labora en las instituciones de BM y de BD, respecto al tema de ingeniería social.

3. Establecer el nivel de conocimiento que tienen los empleados de las instituciones de BM y de BD respecto a los ataques informáticos a los que están expuestos al hacer uso de un equipo de cómputo y telecomunicaciones.

4. Identificar los medios por los cuales los empleados de las instituciones de BM y de BD comparten información según su tipo.

5. Evaluar si la edad, nivel jerárquico y educativo influyen en la divulgación de información.

6. Evaluar si la Ingeniería Social puede contribuir a determinar la cultura de la seguridad de la información en instituciones de BM y de BD en el sector financiero.

JUSTIFICACIÓN

A través de los últimos años se ha observado un incremento considerable en cuanto a fugas de información y fraudes a nivel mundial y, primordialmente, en nuestro país. A raíz de ello las empresas han implantado numerosos mecanismo de seguridad, tanto físicos como lógicos, con la finalidad de incrementar el nivel de seguridad de su información, tratando de evitar con ello dichas fugas que traen como consecuencia los fraudes que hoy en día aquejan a nuestra sociedad.

Cabe aclarar que el activo más importante de una empresa u organización radica en la información; en su compendio residen elementos y datos significativos que al ser comprometidos pueden llegar a generar pérdidas de suma importancia que limiten o comprometan la funcionalidad y continuidad de las empresas.

A sabiendas de ello, resalta una amenaza potencial que de no contar con una cultura referente a la seguridad de la información, así como de valores éticos que conllevan a la misma, es susceptible de revelar la información de manera inconsciente con el simple hecho de mantener una conversación. Dicha amenaza es el factor humano. Pero, ¿cómo podemos saber si determinada persona tiene o no una cultura de seguridad de la información arraigada? ¿Cómo podremos evaluar el nivel de seguridad de la información con la que cuentan las empresas? ¿Cómo se puede implementar la cultura de la seguridad de la información? ¿Existen técnicas que permitan lograrlo?

En un intento por resolver dichas cuestiones, sobresale el concepto del hacking: técnica empleada con el fin de aprovecharse de puntos débiles existentes en un sistema para explotarlos y así demostrar que éste es vulnerable. Desafortunadamente, la mayoría de las personas confunde los conceptos hacker y cracker; por ende, me parece pertinente aclararlo. Hacker es una persona que, como bien lo describe el hacking, se aprovecha de vulnerabilidades existentes para poder perpetuar la seguridad de un sistema con el objetivo de demostrar que pudo hacerlo, a diferencia del cracker, quien realiza exactamente lo mismo, pero con fines maliciosos y lucrativos; éste es precisamente el ente del que comúnmente se habla y teme. Por otro lado, el hacking ético es una auditoría realizada a petición de las organizaciones y en beneficio de éstas, con la finalidad de detectar aquellos puntos débiles que hacen vulnerable a la misma. En consecuencia, se entrega un reporte a la organización con los respectivos hallazgos para que ésta mitigue los fallos y fortalezca su seguridad.

Es bien sabido que el ser humano tiene la necesidad de comunicarse con la finalidad de intercambiar ideas y puntos de vista. Sin la comunicación sería imposible comprendernos y por consiguiente caeríamos en un grave problema. En la mayoría de las ocasiones al momento de sostener una conversación con nuestros amigos o conocidos revelamos datos confidenciales de manera inconsciente, tales como nuestro domicilio, las actividades que realizamos en el trabajo, nuestras fechas de cumpleaños, el nombre de nuestros familiares, el banco en donde se tienen cuentas, los nuevos proyectos que la organización en la que laboramos pondrá en práctica, etcétera. Datos particulares que bien el receptor al que dirigimos la conversación, u otras personas desconocidas que se encuentre escuchando, podrán utilizar para hacer mal uso de ellos. Ésta es precisamente la ingeniería social[1] y su aplicación es un arma poderosa que en ausencia de una cultura referente a la seguridad de la información, primordialmente en las empresas, coadyuvará a que éstas sean un blanco fácil ante posibles ataques, debido a que dicha técnica se aplica al eslabón más débil e importante de la cadena que en la mayoría de las ocasiones es menospreciado, me refiero al "ser humano".

Con lo anteriormente expuesto, el presente trabajo se orienta a profundizar en la investigación, evaluando con ello el impacto que tiene la ingeniería social aplicada como una estrategia de la auditoría del hacking ético en las instituciones mexicanas de Banca Múltiple y de Banca de Desarrollo del Distrito Federal, dentro del sector financiero. Tal impacto determinará el nivel de Seguridad de la Información con el que cuentan dichas empresas y, a sabiendas de ello, en una segunda etapa como continuación de dicha tesis, poder reducir el índice de exposición ante factores que atenten contra la integridad, disponibilidad y confidencialidad de la información; logrando, por consiguiente, implementar una cultura de la seguridad de la información en los empleados que día con día se fortalecerá y se verá reflejada en la consolidación de la organización.

HIPÓTESIS DE TRABAJO

Ho: La Ingeniería Social tiene un papel importante en la seguridad de la información de las instituciones de Banca Múltiple y de Banca de Desarrollo del sector financiero en el Distrito Federal, ya que impacta como medio de prevención y protección; sin embargo, los empleados en el sector tienen conocimientos escasos en la materia, lo que conlleva a una cultura endeble de seguridad generando pérdidas y fugas de información.

[1] Ingeniería social: Es una técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían.

I. LA SEGURIDAD DE LA INFORMACIÓN Y SU RELACIÓN CON EL HACKING ÉTICO– EHTICAL HACKING Y LA INGENIERÍA SOCIAL

1.1 ANTECEDENTES DEL HACKING ÉTICO

En los últimos años ha sobresalido con gran ímpetu el tema del llamado hacking ético y en respuesta a ello han surgido innumerables puntos de vista a favor y en contra del mismo. Seguramente se preguntarán por qué la mayoría de la población parece sucumbir ante la mención de dichas palabras si en la leyenda incluye la palabra "ético" y es bien sabido que el uso de ésta se emplea en términos calificados como "buenos". La respuesta es muy sencilla: se desconoce la labor que realizan los expertos en seguridad de la información[2] al aplicar auditorías de hacking ético, ya que suele confundirse el término y las actividades que realizan los hackers y las que realizan los hackers éticos (dichos términos se aclaran en el capítulo siguiente). Los expertos en seguridad de la información lo único que buscan es el beneficio de las compañías que contratan sus servicios. Sin embargo, un gran porcentaje de la población registra en sus mentes el término del "hacking" como un hecho delictivo y le teme debido a que asocia dicha palabra con la delincuencia cibernética.

Famosos investigadores de virus informáticos y pioneros de la era de la llamada micro computación como Rob Rosenberg y Ross Greenberg afirman categóricamente que "La revolución de la computación se ha logrado gracias a los hackers".

De hecho, de acuerdo a la historia, la primera persona sindicada como "hacker" fue una respetable y sabia mujer. Se trata nada más y nada menos que de la almirante de la Armada de los Estados Unidos Grace Hooper, quien creía firmemente que las computadoras podían servir para aplicaciones en favor de la humanidad y no sólo para el uso que se les daba en los campos científicos y militares.

Fig. 2 Retrato de Grace Hooper, científica informática estadounidense y directora Naval de los EE.UU. Su trabajo incluye la programación de computadoras como la "Harvard Mark I" y el desarrollo del primer compilador para el lenguaje de programación de computadoras. Así mismo, trabajó en la programación de la computadora UNIVAC.[3]

[2] Un experto en seguridad de la información es aquel que realiza la auditoría de *hacking ético.*

[3] UNIVersal Automatic Computer I (Computadora Automática Universal I) fue la primera computadora comercial fabricada en Estados Unidos.

Así que, finalizadas sus labores en el *Bureau of Ordenance Computation*, Hooper se dedicó a investigar las posibilidades de programación en las computadoras de la Primera y Segunda Generación. Sus compañeros comentaban que ella trabajaba como un "hacker", es decir, trabajaba como una persona con un alto nivel de conocimientos en tecnología y podía hacer que ésta funcionara diferente para aquello para lo cual fue diseñada.

Hooper creó el lenguaje Flowmatic, con el cual desarrolló muchas aplicaciones, y en 1951 produjo el primer compilador denominado A-0 (*Math Matic*). En 1960 presentó su primera versión del lenguaje COBOL *(Common Business-Oriented Language)*.

Otros hackers celebres son: Dennis Ritchie y Keneth Thompson quienes desarrollaron, de 1969 a 1971, el famoso sistema operativo UNIX.

Como ellos, muchos otros hackers han hecho, jugando, penetrando y manipulando sistemas, valiosas aportaciones a la computación e incluso, tal y como lo señaló el Dr. Roberto Gómez Cárdenas, experto en seguridad y ex catedrático del Tecnológico de Monterrey, muchos hackers han ayudado a sacar nuevas versiones de sistemas operativos que tenían serios problemas de vulnerabilidad.

Sin embargo, "el término se deformó y terminó por aplicarse a aquellas personas que utilizaban su elevado conocimiento tecnológico para lanzar ataques maliciosos o penetrar los sistemas de las compañías o las instituciones financieras para sacar algún provecho económico", explica el hacker ético Víctor Chapela.

Y dado que en la historia lo malo es comúnmente lo más destacable, el término se satanizó en los medios de comunicación y las noticias de ataques o intrusiones a las cuentas de los bancos se multiplicaron. Así todos aquéllos que utilizaban su habilidad para irrumpir o modificar los sistemas empezaron a cargar con el estigma de entes cibernéticos extraños y maliciosos.

El hacking ético es en sí una auditoría efectuada por profesionales de seguridad de la información quienes reciben el nombre de "pentester" y la auditoría efectuada se denomina con el nombre de "hacking ético" o "pruebas de penetración", dicha auditoría comienza a ser esencial debido al surgimiento de altos índices de delincuencia por fraudes, lo que propicia que las empresas tiendan a mejorar y reforzar la seguridad de sus activos.

Actualmente, existen un sinfín de metodologías para la realización del hacking ético; sin embargo, para fines de esta investigación nos apegaremos al Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM proporcionado por ISECOM.[4] Las pruebas de penetración comienzan a realizarse y expandirse al hacerse presentes los primeros ataques informáticos en las empresas, ataques que fueron efectuados con fines maliciosos y trajeron como consecuencia grandes pérdidas monetarias para las mismas. Es aquí en donde interviene el trabajo de un "hacker ético", ya que su labor es buscar vulnerabilidades en los sistemas de la organización para que posteriormente éstos sean mitigados evitando fugas de información confidencial y vital para la empresa.

[4] ISECOM: Insitute For Security And Open Methodologies.

Hoy en día, desafortunadamente existe un bajo índice de inversión por parte de las empresas en dicha auditoría debido a que no se le presta importancia, se prefiere invertir en otras áreas o simplemente no es del conocimiento de la empresa. Este hecho ha propiciado que las tazas de fraudes se incrementen día a día y año con año de manera exponencial; según un estudio realizado por KPMG, referente a los fraudes en México en el 2010, el nivel de incidencia de fraudes que se registra para 2010 en las compañías que operan en el país es de 75 por ciento, como lo muestra la gráfica de la Fig. 3. Este dato significa que prácticamente 8 de cada 10 empresas que operan en México han padecido cuando menos un fraude en los últimos doce meses. En forma comparada con otros países de la región (Argentina, Brasil, Chile y Uruguay) se puede observar que México sigue presentando los índices de incidencia de fraude más altos, pese a que en varios de estos países se registró un incremento en la incidencia de fraudes, tal y como lo muestra la gráfica de la Fig. 4.

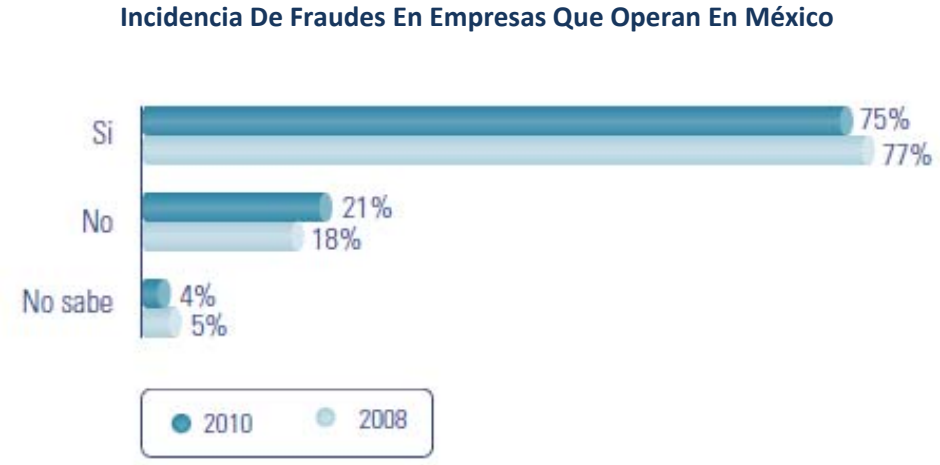


Fig. 3. Gráfica de Incidencia de Fraudes en empresas que operan en México.

Fuente: KPMG. Encuesta de Fraude en México 2010.

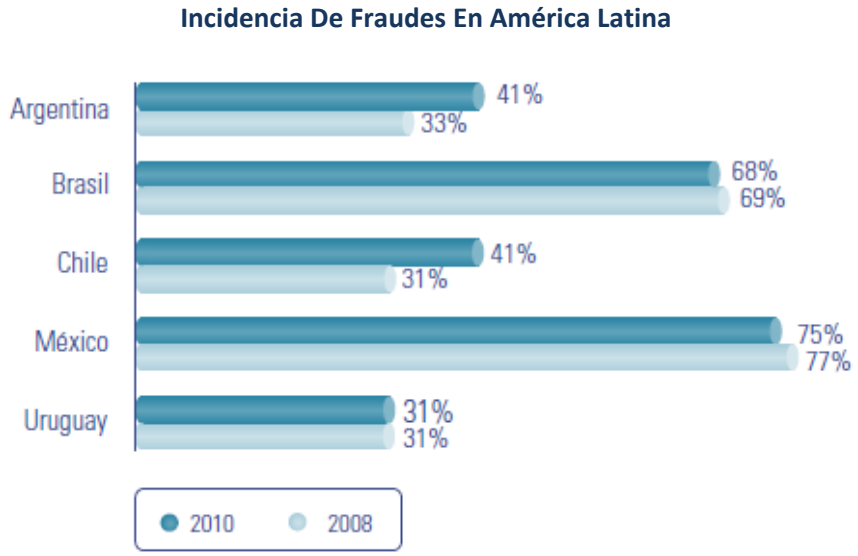


Fig. 4 Incidencia de Fraudes en América Latina
Fuente: KPMG. Encuesta de Fraude en México 2010.

Ahora, si bien es cierto que el nivel de incidencia de fraudes en general se ha mantenido prácticamente en el mismo nivel, lo que sí se puede observar son cambios significativos en el tipo de fraudes cometidos contra empresas que operan en México. En términos de quién comete el ilícito se puede distinguir dos tipos de fraude: el interno y el externo.

El fraude interno es aquél que comete un empleado de la propia organización, sea de manera solitaria o en colusión con alguna otra persona. Por el contrario, el fraude externo es el que realiza una persona ajena a la organización, como puede ser un proveedor o un cliente. Con base en esta clasificación se puede observar que los fraudes que se han cometido en los últimos doce meses a empresas que operan en México son principalmente fraudes internos con un 77 por ciento, como se muestra en la gráfica siguiente (Fig. 5):

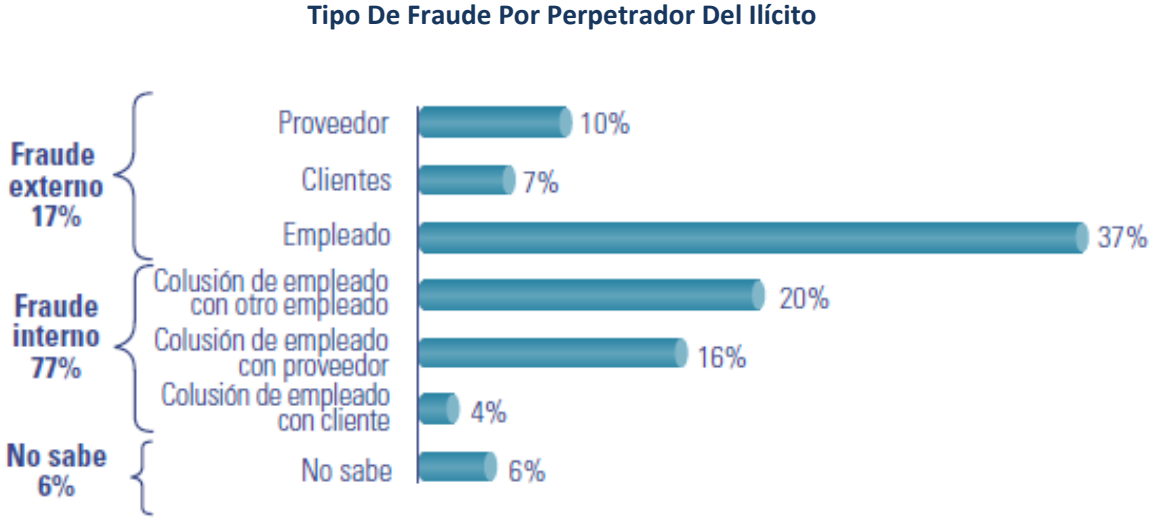


Fig. 5. Tipo de Fraude por perpetrador del ilícito.
Fuente: KPMG. Encuesta de Fraude en México 2010.

Por lo anterior, el control de una empresa debe basarse en un sistema permanente. No se puede dejar el cuidado del patrimonio de la compañía a la buena voluntad ni mucho menos en situaciones de crisis. No olvidemos que en circunstancias como las que hoy se presentan el principal objetivo de las empresas se convierte en mantenerse operativas e impedir mayores pérdidas. De ahí que proteger a la empresa de posibles quebrantos se convierte, en buena medida, en un objetivo estratégico.

Para 2010, sólo 30 por ciento de las compañías que opera en el país han adoptado medidas de prevención de fraudes, fraudes que se pueden deber a fallas en los sistemas, información divulgada consciente o inconscientemente por los trabajadores de las mismas (Dicho tema se abordará con mayor detalle en el Cap. 2), ataques informáticos, falta de cultura organizacional, etcétera. La gráfica siguiente (Fig. 6) muestra la proporción de empresas que cuentan con medidas preventivas y las que reconocen no tenerlas. Esta baja

proporción de empresas con mecanismos de prevención de fraudes explican en parte el nivel de incidencia de fraudes en México, que es uno de los más altos en América Latina.

Porcentaje De Empresas Que Cuentan Con Medidas De Prevención De Fraudes En El 2010

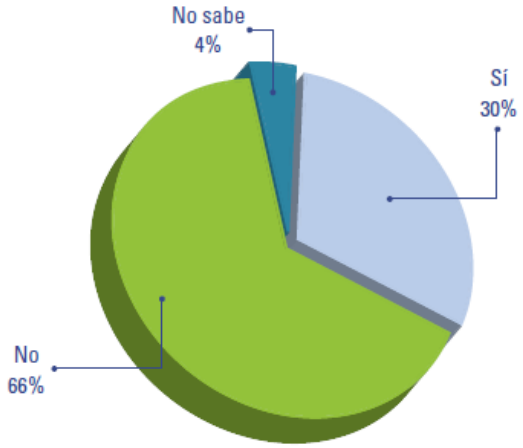


Fig. 6. Porcentaje de empresas que cuentan con medidas de prevención de fraudes en el 2010.
Fuente: KPMG. Encuesta de Fraude en México 2010.

Como se puede observar en la gráfica sólo 4 por ciento de las empresas existentes en nuestro país implementa medidas de prevención de fraude; mientras que el otro 66 por ciento no lo hace y un 30 por ciento no invierte en ello, no porque no quiera, sino debido a que desconoce la existencia de medidas preventivas que ayuden a mitigar la fuga de información confidencial que trae como consecuencia grandes pérdidas monetarias traducidas como fraudes.

Finalmente, me gustaría concluir exponiendo una gráfica en donde de acuerdo con estudios realizados en el 2010 por la Consultora KPMG,[5] se detecta un mayor índice de fraudes de índole interna en las empresas mexicanas.

[5] KPMG es una de las cuatro firmas más importantes del mundo de servicios profesionales junto a PricewaterhouseCoopers, Deloitte Touche Tohmatsu y Ernst & Young. Tiene presencia en 148 países. Es el resultado de la fusión en 1987 entre Klynveld Main Goerdeler (KMG) y Peat Marwick International.

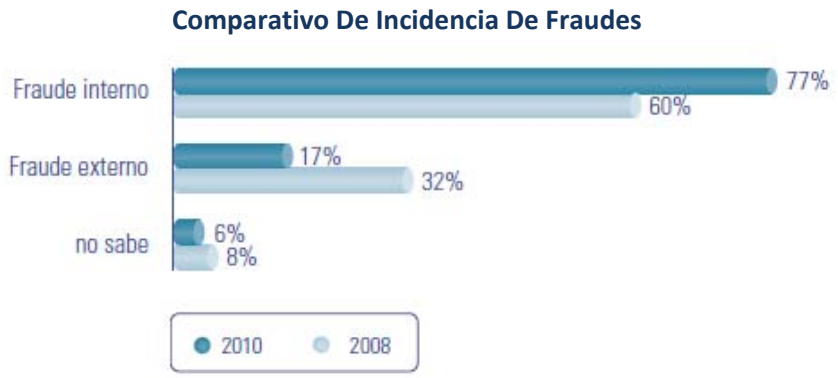


Fig. 7 Comparativo de incidencia de fraudes.
Fuente: KPMG. Encuesta de Fraude en México 2010.

A sabiendas de este hecho, creo conveniente que los empresarios sean conscientes de la gran cantidad de fraudes que acontecen a su alrededor, sobre todo los fraudes internos, los cuales provienen de los mismos empleados que laboran en la organización y que traen consigo información confidencial que revelan a terceros sin percatarse de ello y que éstos últimos pueden emplear de manera inesperada y fatal. Acciones como una simple auditoría de "hacking ético" ayudaría a mitigar dichas fugas de información previniendo el mal uso de la misma y por consiguiente traerá consigo el fortalecimiento de la seguridad de la organización.

1.2 ¿QUÉ ES EL HACKING ÉTICO?

A lo largo de los últimos años han venido sobresaliendo técnicas de intrusión que atentan contra la seguridad de la información que poseen las organizaciones y empresas, involucrando con ello el muy renombrado hacking ético. La mayoría de la población piensa que las pruebas de intrusión o penetración, también conocidas como hacking ético, son dañinas y que por lo tanto hacer uso de la tecnología facilita la aplicación de dicha técnica. Sin embargo, este pensamiento es erróneo.

El hacking ético, o también conocido como pruebas de intrusión o *pentest*, se define esencialmente como el "arte" de comprobar la existencia de vulnerabilidades de seguridad en una organización o empresa que contrató dicho servicio de auditoría para, posteriormente, hacer del conocimiento de la misma y por medio de un informe sobre aquellos fallos de seguridad encontrados para que sean mitigados a la brevedad posible, evitando con ello fugas de información y por consiguiente ser víctimas de ataques informáticos.

Pese a su mala fama, no todos los hackers son delincuentes cibernéticos, pues algunos ayudan a las empresas a reforzar su seguridad. Es por ello que, tratando de diferenciar a un grupo de otro, se introdujo el término crackers, para identificar a aquellos entes que realizan técnicas de intrusión con fines maliciosos y lucrativos, y hackers éticos para quienes lo hace con la finalidad de demostrarse que pudieron hacerlo o bien con fines éticos y para el bien de la organización o empresa que los contrate; de ahí que provenga el nombre de hacking ético. Aunque también se generó una segmentación más al estilo de los dos bandos donde existe, dentro del término hacker, el grupo que se mueve en el lado obscuro, a quienes también se les conoce como los hackers de "sombrero negro o Black Hat", y el otro ubicado en el bando de los buenos o también llamados hackers de "sombrero blanco o White Hat".

Los hacker de sombrero negro, mejor conocidos como "Black Hat", tienen la cualidad de explotar vulnerabilidades en los sistemas con la finalidad de demostrarse que lo pudieron hacer burlando la seguridad del mismo, ejemplo de ello lo tenemos en el muy reciente caso, acontecido en febrero del 2008, que se presentó en la página web oficial de la Presidencia de la República en donde un hacker, protegido con la identidad de H4t3 M3, decidió dejar la huella de una imagen de lo más elocuente debido a que esa página web tenía una vulnerabilidad. La información fue revelada en el foro de la Comunidad Underground Latinoamericana www.hackeruna.com, en dónde el joven hacker advirtió que podía modificar desde la agenda presidencial hasta las noticias, pero que no creía hacerles nada.

Por otro lado, los hackers de sombrero blanco o "White Hat", también conocidos como hackers éticos, pentesters y expertos en seguridad, tienen la finalidad de realizar pruebas de intrusión en empresas u organizaciones que así lo pidan, para posteriormente rendirles un informe en el cual se detallan todos aquellos puntos vulnerables encontrados y de los cuales se aprovecharon para que, posteriormente, la empresa los mitigue a la brevedad posible evitando con ello fugas de información confidencial. Ejemplo de ello lo tenemos con los Consultores de Seguridad cuya especialidad es la realización de pruebas de penetración en empresas u organizaciones que así lo solicitan.

A continuación se describe dicha clasificación en la siguiente ilustración:

Clasificación de los entes que realizan ataques de intrusión

Fig. 8. Clasificación de sujetos que realizan pruebas de intrusión.
Fuente: Elaboración propia.

Cuando en 1997 la cultura de la seguridad informática comenzó a tomar fuerza, se pensó en que los hackers éticos podían ofrecer sus servicios a las empresas para ayudarlas a ser menos vulnerables y en el 2001 arrancaron en forma este tipo de asesorías.

Así los hackers blancos, ya sea trabajando individualmente, dentro de una empresa bien organizada o dentro de diversas consultoras, comenzaron a ofrecer sus servicios "para ayudar a las compañías a encontrar fallas y actuar en consecuencia", precisa Luis Guillermo Castañeda, consultor en seguridad.

Pese a esta segmentación, la sola palabra hacker impone, porque finalmente no hay una escuela donde se aprenda a penetrar los sistemas, eso sólo se logra con la práctica. De manera que tanto un bando como el otro han realizado en algún momento intrusiones sin permiso.

Tal y como lo explica Luis Alberto Cortés, consultor en seguridad y hackeo ético, se tienen que haber penetrado sistemas, jugado con ellos y poseer la malicia para encontrar la técnica más apropiada o inventar nuevas maneras para entrar. La diferencia aquí es que algunos iniciamos haciendo esto por diversión, como una forma de vencer un reto y probar nuestros conocimientos, pero sin causar daño y otros lo hacen para descubrir vulnerabilidades y lanzar ataques, ya sea para obtener un beneficio económico o para poder jactarse de que lograron burlar las medidas de seguridad de una empresa.

Convencer a las compañías de contratar un hacker, por mucho que se llame ético, y conseguir el permiso para penetrar y jugar con sus sistemas no ha sido fácil. “No puedes llegar y simplemente decir te ofrezco un *hackeo ético*, debes explicar muy bien qué es esto y cuáles son los objetivos”, comenta Cortés.

Sobre tal punto, el término poco a poco se ha ido aceptando, tan es así que los clientes ya empiezan a conocer a los hackers éticos y buscan sus servicios. Por otra parte, las grandes empresas de seguridad como Ernest & Young o PriceWaterhouse han empezado a ofrecer servicios de hackeo ético, lo cual ayuda a generar mayor confianza en este tipo de asesoría.

Asimismo, se ha desarrollado alrededor de todo esto una especie de código de honor y contratos especiales que se firman entre los hackers blancos o hackers éticos y las compañías usuarias, para mayor protección de estas últimas. En dicho contrato se estipula que la empresa da permiso para realizar la intrusión, se marca el lapso de duración de las pruebas correspondientes, disponibilidad de fechas para hacerlos y la forma en cómo se van a entregar los resultados, que generalmente es a manera de un reporte, donde se enumeran las vulnerabilidades y fallas encontradas, así como las recomendaciones para mitigar los problemas y optimizar la seguridad.

Aunado a ello, se incluye una cláusula de confidencialidad en donde se enuncia que todos aquellos hallazgos de vulnerabilidades encontrados en la empresa u organización a raíz de las pruebas de penetración, no podrán ser divulgadas por el hacker a otra entidad que no sea la compañía misma que contrató sus servicios, ni tampoco se podrá quedar con una copia del reporte final generado para la empresa, esto con la finalidad de evitar que la información revelada se exponga a terceros que podrían hacer mal uso del a información. De no cumplir con dicho estatuto el hacker se haría acreedor a una demanda.

En conclusión, el hacking ético es una técnica aplicada a distintos escenarios que en su conjunto permiten entregar resultados sustanciales a las organizaciones por parte de los profesionales de seguridad mejor conocidos como *pentesters* (hackers éticos), cuya labor es detectar y explotar vulnerabilidades existentes en una infraestructura de red, para posteriormente generar un informe con los hallazgos encontrados así como las recomendaciones pertinentes para la mitigación de los mismos.

Es importante hacer del conocimiento de la gente la diferencia que existe entre los términos hacker y cracker, ya que se prestan a confusión y se juzga al ente incorrecto; por ello exhorto a todo los lectores a que no hagan caso omiso de lo que aquí se expone para que al referirse a delincuentes informáticos no se relacione directamente con los hackers ni piensen que dicha palabra es un término malo. Sino al contrario, el hacker, pero sobre todo el hacker ético, ayuda a encontrar puntos vulnerables de ataques informáticos, evitando que los crackers se aprovechen de ellos y causen daños y estragos graves en perjuicio de las personas físicas y morales.

1.3 SECCIONES A EVALUAR EN UNA AUDITORÍA DE HACKING ÉTICO SEGÚN EL OSSTMM- OPEN SOURCE SECURITY TESTING METHODOLOGY MANUAL

Los servicios que con mayor frecuencia ofrecen los hackers blancos (hackers éticos) a las empresas son las pruebas de penetración, con la intención de analizar si la compañía está preparada para soportar un ataque sofisticado perpetrado desde fuera, es decir por un hacker externo o por un atacante interno con conexión a la red.

Durante las pruebas de penetración, según enumera Víctor Chapela, se analizan: la red de Internet, aplicaciones expuestas, servidores, puertos y avenidas de acceso, además se hacen pruebas de contraseñas. Al mismo tiempo se analiza la red inalámbrica, de ésta se revisa la configuración, se hace *sniffing*[6] de tráfico y contraseñas, se intenta penetrarla y romper cifrado.

También se pone bajo la lupa a la red interna, en donde se intenta, la penetración, se prueban contraseñas, se analizan vulnerabilidades en servidores y aplicaciones, así como avenidas de acceso.

Parte de la auditoría incluye también revisar módems, VPN, página web, DMZ e incluso se *hace ingeniería social*, es decir *se trabaja con el personal o con los asociados de la empresa para ver si se dejarían engañar para proporcionar contraseñas o acceso a la red.*

De igual forma se mide el nivel de respuesta a incidentes internos, también se busca emular si un empleado de bajos privilegios podría tener acceso a los estados financieros o a la nómina de la compañía. Se consideran además los valores de los activos, la criticidad de la vulnerabilidad y la probabilidad del ataque, su impacto, la forma de corregirlo y el esfuerzo requerido para esto.

Claro que para evitar cualquier contratiempo o daño a la infraestructura o continuidad de negocio del cliente, tales pruebas siguen una metodología y manejan estándares, como Manual de la Metodología Abierta de Comprobación de la Seguridad (*OSSTMM*, por sus siglas en inglés) o el Proyecto Abierto de Seguridad de Aplicaciones Web *(OWASP)*, para reducir riesgos y evitar las fugas de información.

Para fines de éste trabajo, según el Mapa de Seguridad propuesto por manual de la metodología abierta de testeo de seguridad, de sus siglas en inglés *OSSTMM-Open Source Security Testing Methodology Manual*,[7] las secciones a las cuales se aplican el hacking ético son las siguientes:

Mapa De Seguridad Según OSSTMM 2.1

[6] Sniffing: Se trata de una técnica por la cual se puede "escuchar" todo lo que circula por una red. Esto que en principio es propio de una red interna o Intranet, también se puede dar en la red de redes “Internet”.

[7] Herzog, Pete (2003). “OSSTMM 2.1”, *Manual de la Metodología Abierta de Testeo de Seguridad*. USA: ISECOM Institute for Security and Open Methodologies. Recuperado el 30 de septiembre de 2010, http://www.isecom.org/research/osstmm.html

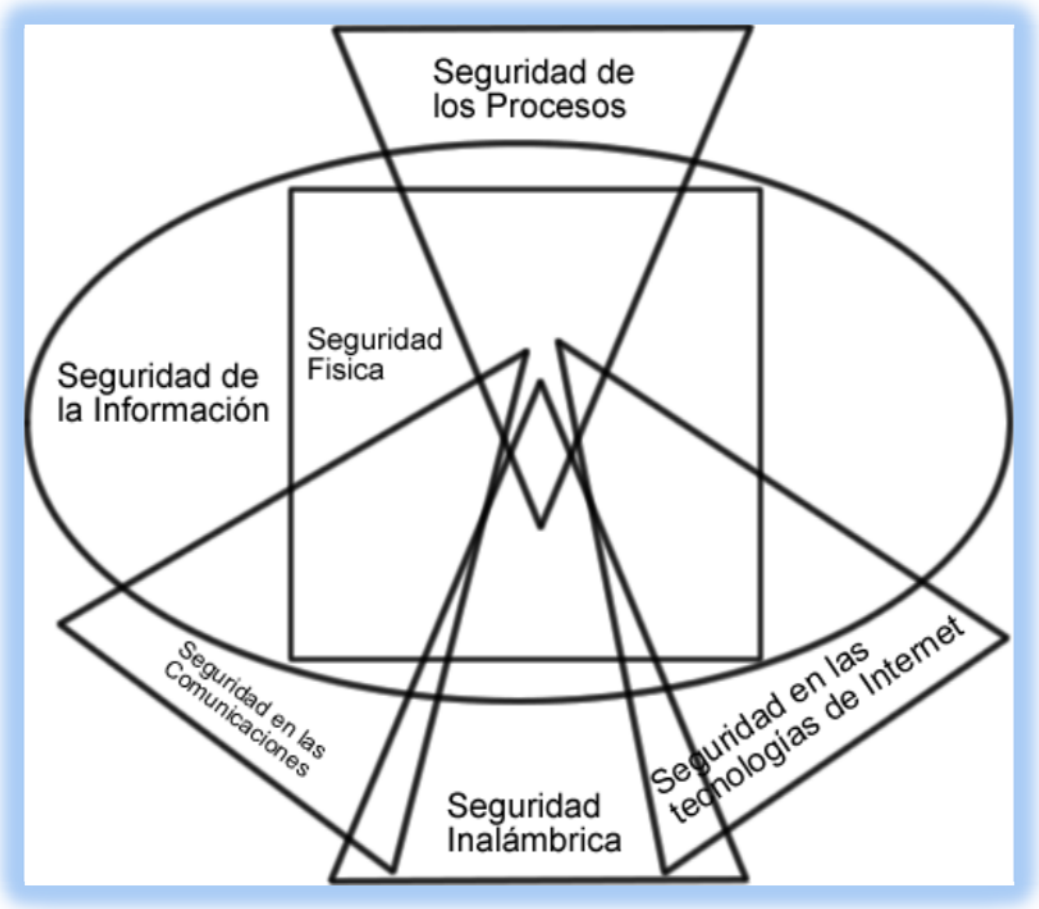


Fig. 9. Mapa de Seguridad
Fuente: Tomado del *Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM 2.1* de ISECOM.

Cabe destacar que, como se muestra en la ilustración, el mapa de seguridad es una imagen de la presencia de seguridad. Esta corresponde al ambiente de un análisis de seguridad y está compuesta por seis secciones equivalentes según el manual OSSTMM. Como se puede observar, las secciones se superponen entre sí y contienen elementos de todas las otras secciones; se considera que un análisis apropiado de cualquier sección debe incluir los elementos de todas las otras secciones, ya sea de manera directa o indirectamente.

A continuación se describen cada una de las secciones.

1.3.1. SEGURIDAD FÍSICA

Dicha sección alude a las pruebas de seguridad realizadas que refieran a un medio físico y no electrónico en la naturaleza. Comprende el elemento tangible de la seguridad donde la interacción requiere un esfuerzo físico o una transmisión de energía para que sea manipulado. Los módulos de verificación requeridos en el hacking ético para dicho rubro son:

Fig. 10. Módulos de verificación para la Sección de Seguridad Física.
Fuente: *Elaboración propia con base en el Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM 2.1* de ISECOM.

1.3.2. SEGURIDAD EN LAS COMUNICACIONES

Dicho rubro comprende dos fases: Telecomunicaciones y las redes de datos. La primera fase alude a todas las redes de telecomunicación tanto digitales como analógicas, donde la interacción se realiza a través de la telefonía establecida o líneas de red como el teléfono; por otra parte, en lo que respecta a las redes de datos, se refiere a todos los sistemas electrónicos y redes de datos donde la interacción se realiza a través de cables establecidos y cables de líneas de red así como redes de datos. Los módulos de verificación requeridos en el hacking ético para dicho rubro se muestran a continuación:

Módulos De Verificación Para La Sección De Seguridad En Las Comunicaciones

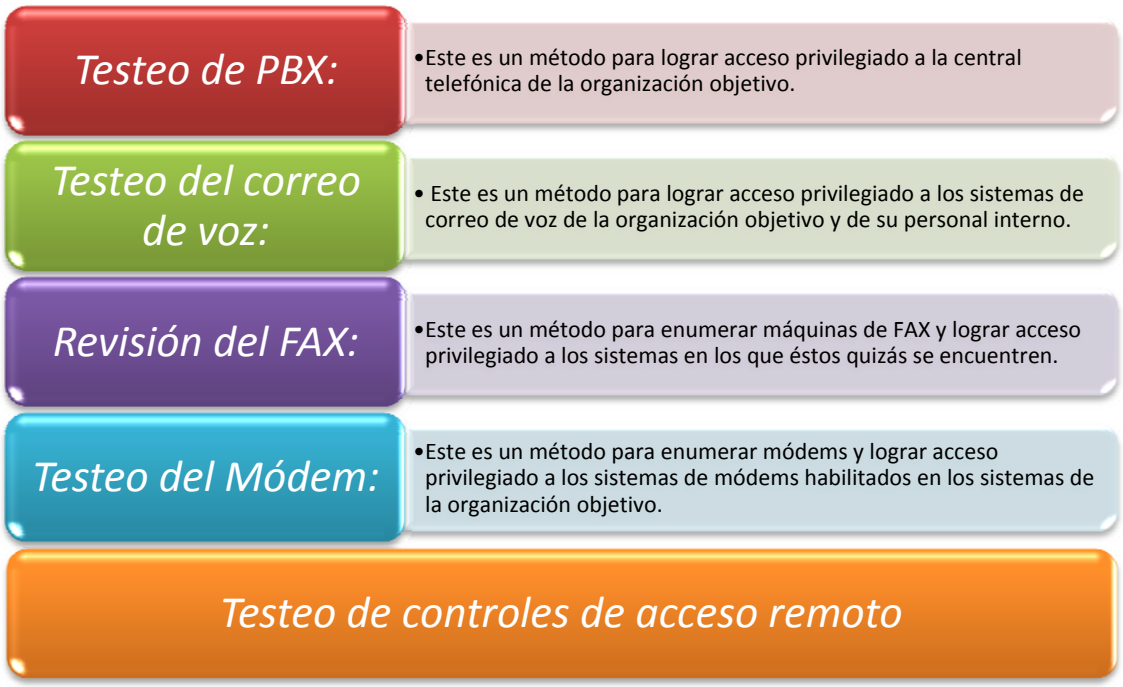


Fig. 11. Módulos de verificación para la Sección de Seguridad en las Comunicaciones.
Fuente: Elaboración propia con base en el *Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM 2.1* de ISECOM.

1.3.3. SEGURIDAD EN LAS TECNOLOGÍAS DE INTERNET

Dicho rubro alude las pruebas de intrusión efectuadas a las aplicaciones web, tales pruebas son esencialmente el "arte" de comprobar una aplicación en ejecución remota o local, sin saber el funcionamiento interno de la aplicación, para encontrar vulnerabilidades de seguridad.[8] Así como la revisión de vulnerabilidades existentes en los equipos de cómputo con los que cuenta la organización, mejor conocidos como "hosts" y los dispositivos de red empleados. Los módulos de verificación requeridos en el hacking ético para dicho rubro son:

[8] OWASP Foundation (2008). *Guía de pruebas OWASP versión 3.0*. USA: OWASP The open Web Application Security Project. Recuperado el 29 de abril de 2012, https://www.owasp.org/index.php/Category:OWASP_Testing_Project

Módulos de verificación para la sección de seguridad física

Logística de Controles:	•El propósito de este módulo es reducir los falsos positivos y negativos realizando los ajustes necesarios en las herramientas de análisis.
Sondeo de Red:	•El sondeo de red sirve como introducción a los sistemas a ser analizados. Se podría definir mejor como una combinación de recolección de datos, obtención de información y política de control.
Identificación de los servicios de sistemas:	•El escaneo de puertos es la prueba invasiva de los puertos del sistema en los niveles de transporte y red. También se incluye aquí la validación de la recepción del sistema a protocolos tunelizados, encapsulados o de enrutamiento. En éste módulo se enumerar los servicios de Internet activos o accesibles así como traspasar el cortafuegos o también denominado firewall con el objetivo de encontrar más máquinas activas.
Búsqueda de información competitiva:	•La Búsqueda de IC es la búsqueda de información útil a partir de la presencia que se tiene en Internet y que puede ser tratada como información sobre el negocio.
Revisión de privacidad:	•La revisión de privacidad se centra en cómo se gestiona, desde un punto de vista ético y legal, el almacenamiento, transmisión y control de datos de información privada perteneciente a empleados y clientes.
Obtención de Documentos:	•Este módulo es importante para la verificación de gran cantidad de la información probada y pertenece a muchos de los niveles de lo que se considera seguridad de la información.
Búsqueda y verificación de vulnerabilidades:	•La finalidad de este módulo es la identificación, comprensión y verificación de debilidades, errores de configuración y vulnerabilidades en un servidor o en una red.

Testeo de aplicaciones de internet:	•Un test de Aplicaciones de Internet emplea diferentes Técnicas de testeo de Software para encontrar "fallos de seguridad" en aplicaciones cliente/servidor de un sistema desde Internet. En este módulo, se refiere a aplicaciones cliente/servidor que sean desarrolladas por los administradores de sistema con propósitos de la empresa y programadas con cualquier tecnología y lenguaje de programación.
Enrutamiento:	• Las Protecciones de un Router son unas defensas que se encuentran a menudo en una red donde se restringe el flujo del tráfico entre la red de la empresa e Internet. Opera en una política de seguridad y usa ACL's (Access Control Lists o Lista de Control de Acceso) que acepta o niega paquetes. Este módulo está diseñado para asegurar que solo aquello que debe ser expresamente permitido, puede ser aceptado en la red; todo lo demás debe ser rechazado.
Testeo de sistemas confiados:	•El propósito de los testeos de sistemas confiados es afectar la presencia en Internet planteándose como una entidad confiada en la red. El escenario de testeo es a veces más teoría que práctica, y en realidad más que oscurecer la frontera entre un Test de Vulnerabilidad y un Testeo de Firewall / Listas de control de acceso ACLS, es dicha frontera.

Testeo de control de acceso:

- El cortafuegos o firewall controla el flujo del tráfico de la red corporativa, la DMZ e Internet. Opera en una política de seguridad y usa ACL's (Listas de Control de Acceso). Este módulo está diseñado para asegurar que solo lo que debe estar expresamente permitido puede ser aceptado dentro de la red, todo lo demás debe ser negado.

DMZ:

- Una zona desmilitarizada (**DMZ, demilitarized zone**) o red perimetral es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet.

Testeo de Sistema de Detección de Intruso IDS:

- Este test está enfocado al rendimiento y susceptibilidad de un Sistema de detección de intrusos de sus siglas en inglés IDS- Intrusion Detection System. La mayor parte de este test no puede ser llevada a cabo adecuadamente sin acceder a los registros del IDS. Algunos de estos tests están relacionados con ataques de ancho de banda, saltos distantes y latencia que afectan al resultado de estas pruebas.

Testeo de Medidas de Contingencia:

- Las medidas de contingencia dictan el manejo de lo atravesable, programas maliciosos y emergencias. La identificación de los mecanismos de seguridad y las políticas de respuesta que necesiten ser examinados.

Descifrado de contraseñas:

- Descifrar las contraseñas es el proceso de validar la robustez de una contraseña a través del uso de herramientas de recuperación de contraseñas automatizados, que dejan al descubierto la aplicación de algoritmos criptográficos débiles, implementaciones incorrectas de algoritmos criptográficos, o contraseñas débiles debido a factores humanos.

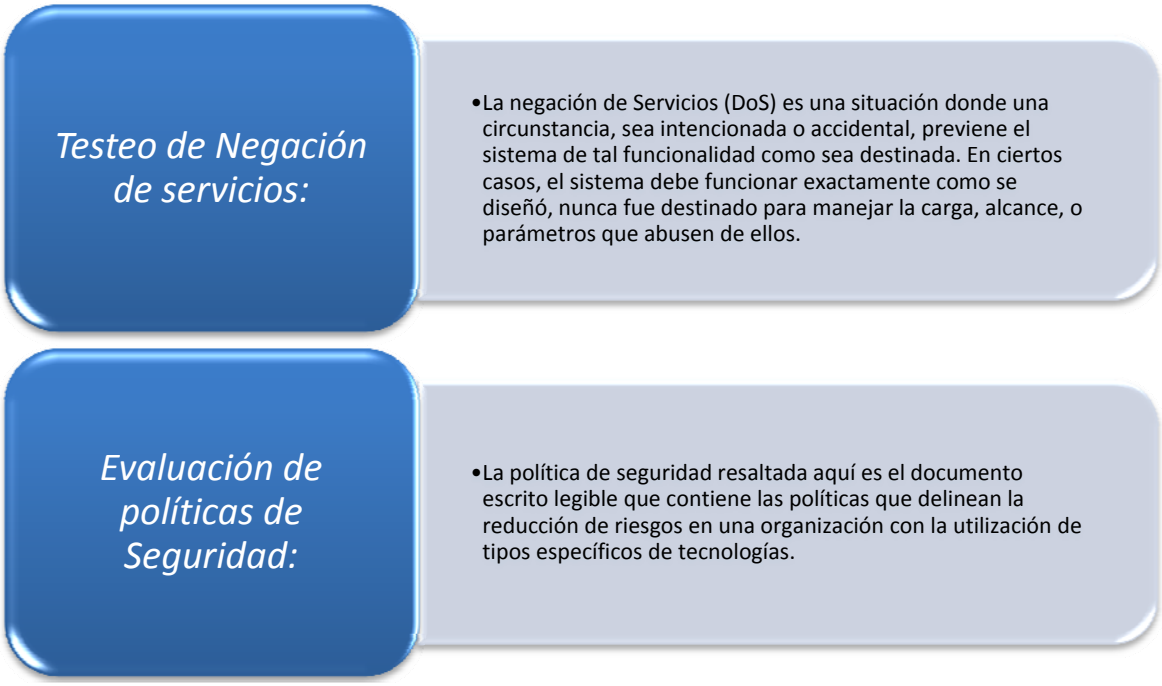


Fig. 12 Módulos de verificación para la Sección de Seguridad Física.
Fuente: Elaboración propia con base en el *Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM 2.1* de ISECOM.

1.3.4. SEGURIDAD INALÁMBRICA

Comprende todas las comunicaciones electrónicas, señales y emanaciones que se producen del conocido espectro *EM – Electromagnetic*. Esto incluye ELSEC como comunicaciones electrónicas, SIGSEC como señales, y EMSEC que son emanaciones sin ataduras por los cables. Los módulos de verificación requeridos en el hacking ético para dicho rubro son:

Módulos de verificación para la sección de seguridad inalámbrica

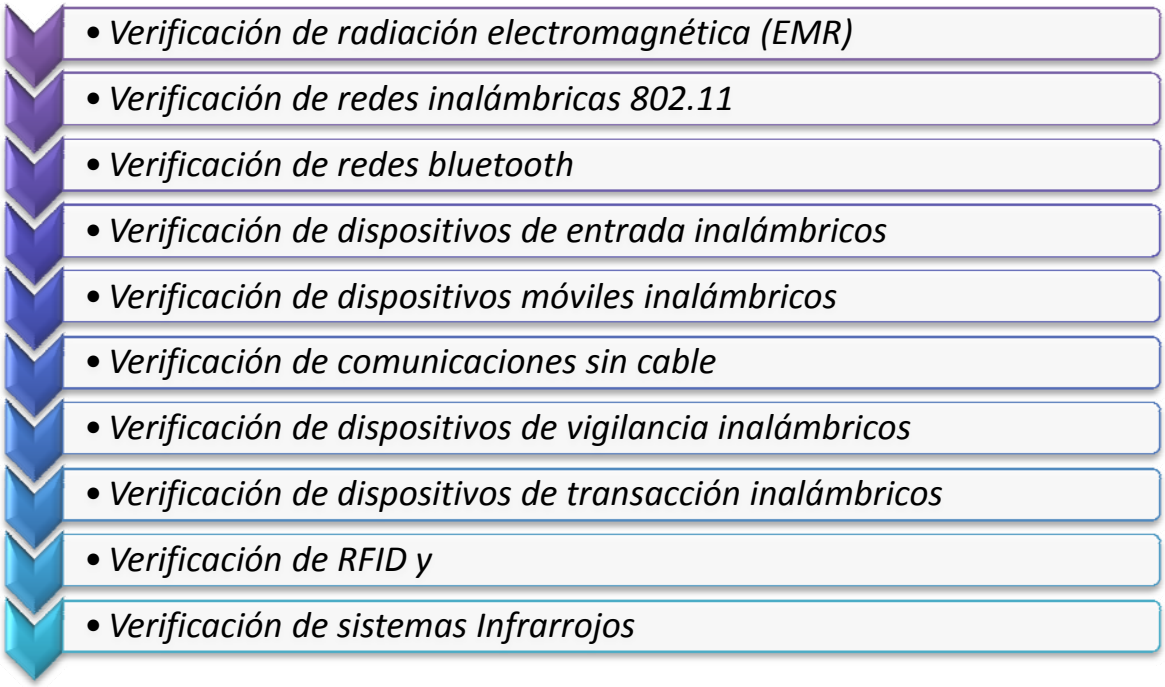


Fig. 13. Módulos de verificación para la Sección de Seguridad Inalámbrica.
Fuente: Elaboración propia con base en el *Manual de la Metodología Abierta de Testeo de Seguridad OSSTMM 2.1* de ISECOM.

1.3.5. SEGURIDAD DEL RESGUARDO DE INFORMACIÓN

En dicho rubro se alude a los medios empleados para el almacenamiento adecuado de la información y va ligado con los controles empleados para su seguridad.

1.3.6. CAPACITACIÓN EN MATERIA DE SEGURIDAD INFORMÁTICA Y SU RELACIÓN CON LA INGENIERÍA SOCIAL

En este rubro la aplicación del hacking ético se emplea por medio de la práctica de la ingeniería social, la cual es una técnica especializada o empírica del uso de acciones estudiadas o habilidosas que permiten manipular a las personas para que voluntariamente realicen actos que normalmente no harían.[9]

[9] Mitnick, Kevin. (2002). *Controlling the Human Element of Security. The Art Of Deception*. USA: John Wiley & Sons Australia.

Precisamente, este último rubro es el que se pretende explotar en dicha investigación, demostrando que con una divulgación adecuada en las organizaciones referente a la cultura de la seguridad de la información se evitarán fugas desmesurables de este importante activo, asegurando con ello la integridad y confidencialidad de la información contenida en la organización, así como de los recursos humanos que en ella laboren.

1.3.6.1 PLANTILLAS PARA EL VACIADO DE DATOS UNA VEZ APLICADA LA INGENIERÍA SOCIAL SEGÚN LA OSSTMM 2.1

Plantilla de ingeniería social

OSSTMM 2.1. –Manual de Metodología Abierta de Testeo de Seguridad
23 de agosto de 2003

ISECOM Institute for Security and Open Methodologies

Plantilla de Ingeniería Social sobre el Objetivo

Definición del Objetivo

Nombre	Correo electrónico	Teléfono	Descripción

Fig. 14. Plantilla de Ingeniería Social sobre el Objetivo.
Fuente: Tomado del Institute for Security and Open Methodologies ISECOM (2003). *Manual de Metodología Abierta de Testeo de Seguridad OSSTMM 2.1*.

Plantilla para el vaciado de datos derivado de un ataque telefónico usando la técnica de la ingeniería social

Plantilla de Ataque Telefónico usando Técnicas de Ingeniería Social

Escenario de ataque	
Número de teléfono:	
Persona	
Descripción	
Resultados	

Escenario de ataque	
Número de teléfono:	
Persona	
Descripción	
Resultados	

Fig. 15. Plantilla para el vaciado de datos derivado de un ataque telefónico usando la técnica de la Ingeniería Social. Fuente: Tomado de Institute for Security and Open Methodologies ISECOM (2003). *Manual de Metodología Abierta de Testeo de Seguridad OSSTMM 2.1.*

Plantilla de vaciado de datos derivados de un ataque por correo electrónico usando la técnica de la ingeniería social

Plantilla de Ataque por Correo Electrónico usando Técnicas de Ingeniería Social

Escenario de ataque	
Correo electrónico:	
Persona	
Descripción	
Resultados	

Escenario de ataque	
Correo electrónico:	
Persona	
Descripción	
Resultados	

Fig. 16. Plantilla de vaciado de datos derivados de un ataque por Correo Electrónico usando la técnica de la Ingeniería Social.

Fuente: Tomado de Institute for Security and Open Methodologies ISECOM (2003). *Manual de Metodología Abierta de Testeo de Seguridad OSSTMM 2.1*.

Plantilla de Ingeniería Social

Compañía	
Nombre de la compañía	
Dirección de la compañía	
Teléfono de la compañía	
Fax de la compañía	
Página web de la compañía	
Productos y Servicios	
Contactos Principales	
Departamentos y Responsabilidades	
Ubicación de las oficinas	
Historia de la Compañía	
Socios	
Revendedores	
Regulaciones de la compañía	
Información sobre políticas de seguridad	
Tradiciones de la compañía	
Publicación de ofertas de trabajo	
Disponibilidad de empleos temporales	
Riesgos típicos de IT	

Personas	
Información de empleados	
Nombre y cargos de empleados	
Posición del empleado en la jerarquía	
Páginas personales del empleado	
Métodos de contacto del empleado	
Pasatiempos del empleado	
Datos en Internet del empleado (listas de correo, usenet)	
Opiniones que ha expresado el empleado	
Familiares y amigos del empleado	
Historial del empleado (incluyendo historia laboral)	
Rasgos del carácter del empleado	
Valores y prioridades del empleado	
Hábitos sociales del empleado	
Patrones de habla y forma de hablar del empleado	
Gestos y maneras del empleado	

Equipamiento	
Equipamiento utilizado	
Servidores, número y tipo	
Estaciones de trabajo, número y tipo	
Programas utilizados (y versiones)	
Nombres de host utilizados	
Topología de red	
Capacidades anti-virus	
Recursos usados para la protección de la red (con sus versiones de software)	
Recursos usados para acceso remoto (incluyendo conexión por modem)	
Routers utilizados (con sus versiones de software)	
Tecnología usada para el control de acceso físico	
Ubicación de los vertederos de desechos utilizados	

Fig. 17. Plantilla de Ingeniería Social.

Fuente: Tomado de Institute for Security and Open Methodologies ISECOM (2003). *Manual de Metodología Abierta de Testeo de Seguridad OSSTMM 2.1.*

Como lo hemos visto a la largo del Capítulo I, se han abordado aspectos relevantes respecto de la historia del Hacking Ético, sus antecedentes, roles que juegan los indiviso al aplicar dicha técnica, así como las secciones que se evalúan para efectuar una auditoria de ésta índole según el manual *OSSTMM (Open Source Security Testing Methodology Manual)*propuesto por *ISECOM (Institute for Security and Open Mehtodologies)* para evaluar la vulnerabilidad de los sistemas y controles de seguridad tanto físicos, lógicos y de la información que sustentan las organizaciones con la finalidad de evitar fugas de información y ataques informáticos que atenten contra su seguridad.

A partir de esto, iniciaremos con el tema de la Ingeniería Social, que es un factor y una vertiente importante del Hacking Ético en el estudio abordado.

II. LA INGENIERÍA SOCIAL

Como se menciona en el Capítulo I, la Ingeniería Social forma parte importante de una Auditoría de Hacking Ético y se abordará ampliamente en éste capítulo.

El mundo de la seguridad de la información está siempre en evolución, los hackers y crackers constantemente desarrollan maneras de evitar las medidas de seguridad multi-capa que las organizaciones establecen en su perímetro, usando para ello nuevos vectores de ataque altamente sofisticados, creativos y devastadores. Es por ello que, como profesionales de la seguridad, necesitamos estar un paso adelante para ayudar a los clientes a reducir sus riesgos y a mejorar la postura de seguridad de sus organizaciones.

La seguridad hoy en día no es sólo una cuestión técnica que se solucione con firewalls, detectores de intrusos, sistemas contra pérdida y robo de información, sistemas de seguridad Web o con la última campaña de medidas antispam; la seguridad es una cuestión que tiene que ver con la gente. Las personas somos el eslabón más débil en el sistema de seguridad y mientras las empresas alrededor del mundo gastan millones de dólares en dispositivos como firewalls, procesos de autenticación y software para monitoreo de redes, pocas se preocupan por capacitar a sus empleados para evitar que terceros obtengan, indebidamente, información crítica y confidencial de ellos.

A pesar de todas las defensas tecnológicas, los hackers y crackers pueden "esquivar" la seguridad de una organización con sólo enfocar su atención en los empleados para llevar ataques con un método llamado "ingeniería social". El reto aquí es que la ingeniería social es real y altamente efectiva porque se concentra en explotar la mayor vulnerabilidad: la gente. Este vector de ataque puede anular los sistemas técnicos más efectivos mediante la manipulación de las personas con técnicas de engaño.

2.1 ¿QUÉ ES LA INGENIERÍA SOCIAL?

La ingeniería social es una colección de técnicas empleadas para manipular a la gente y hacer que divulgue información confidencial. El término se aplica a la recopilación de datos sobre sistemas informáticos por medio de engaño.

Para los hackers, crackers, espías industriales, investigadores privados, periodistas y otros, la ingeniería social es un método muy atractivo para obtener acceso a información valiosa. Además de efectiva, es una alternativa de bajo riesgo en comparación con los métodos de hacking tradicionales que buscan la penetración de los sistemas y redes por medios técnicos y, finalmente, es una ruta rápida que evita tener que implantar ataques sofisticados en el perímetro de seguridad de una organización.

La Ingeniería social se define como el proceso de engañar a la gente para que den acceso a información confidencial. En la mayoría de los casos se define como el acto de manipular a la gente para realizar acciones o divulgar información confidencial. Aunque es similar a una estafa o fraude simple, el término se aplica normalmente al engaño o el engaño con el propósito de la recopilación de información, realización de fraude o acceso al sistema informático. En la mayoría de los casos el atacante nunca se encuentra cara a cara con la víctima.

Actualmente, la ingeniería social toca muchos aspectos de la vida diaria y es considerada, por la mayoría de los profesionales en seguridad, como el *mayor riesgo que atenta contra la seguridad*.[10]

El famoso consultor de seguridad y ex-hacker Kevin Mitnik define la Ingeniería Social como: "Una forma de hacking que se basa en influenciar, engañar y manipular psicológicamente a la gente para que inconscientemente cumpla una solicitud". Por su parte, para Microsoft: "El objetivo de un hacker que emplea Ingeniería Social, alguien que trata de obtener acceso no autorizado a sistemas de cómputo, es similar al de cualquier otro tipo de HACKER: quiere el dinero, la información o los recursos de TI de una organización" (Hinson, 2006).[11] Cabe aclarar que con respecto a este punto de vista, estoy en total desacuerdo debido a que, como se definió previamente en el Capítulo I, existe una diferencia muy remarcada entre el hacker y el cracker y esta diferencia radica en las acciones que dichos entes realizan, para ello recordemos que el cracker es quien realiza las acciones con fines lucrativos mal habidos y maliciosos, mientras que el hacker simplemente lo hace para demostrarse y demostrar a los demás que pudo burlar las medidas de seguridad de una empresa u organización.

Aunado a ello, recordemos que los hackers se dividen en aquellos de sombrero negro (Black hacker) y aquellos de sombrero blanco (White hacker), ambos cuyas acciones son realizadas para burlar la seguridad de las organizaciones; sin embargo, los black hackers lo hacen con fines maliciosos para demostrar la escases de medidas de seguridad de la empresa u organización, mientras que los white hackers o también llamados hackers éticos o *pentester* lo hacen con base en un convenio con la empresa u organización para, una vez concluidas las pruebas correspondientes, presentar un reporte a la misma con aquellos hallazgos que hayan surgido en la auditoría para que la organización o empresa mitigue las fallas a la brevedad posible.

Asimismo, cabe destacar que el hacker ético*, pentester o* white hacker, recibe cierta remuneración en pago por sus servicios durante la ejecución de la auditoría correspondiente con el consentimiento de la misma empresa u organización. Por otro lado, el black hacker no recibe dicha remuneración. Sin embargo, ambos entes no persiguen la finalidad del lucro mal habido como lo hace el cracker y es de suma importancia que quede claro dicho punto, ya que se puede prestar a confusión debido a lo que comenta Microsoft.

A sabiendas de que la Ingeniería Social puede incluir la seguridad física, este trabajo de investigación se centra en el arte de manipular a la gente para lograr un objetivo. La meta consistirá en mostrar a una empresa u organización el lugar en donde puede yacer su debilidad a falta de la capacitación de su personal para que éste pueda mantener una visión de seguridad al día y a la vanguardia.

[10] Kotadia, Munir (2004). Greates Security Risk: Social Engineering. ZDNet UK Recuperado el 25 de septiembre de 2011 en http://www.social-engineer.org/wiki/archives/SEDefined/SEDefined-GreatestRisk.htm

[11] Hinson, Gary (2008). Social Engineering Techniques, Risks, and Controls. EDPACS: The EDP Audit, Control, and Security Newsletter.37(4-5), 32-36. Recuperado el 30 de septiembre de 2011 en http://www.tandfonline.com/doi/abs/10.1080/07366980801907540

2.2 ¿QUIÉNES SON VULNERABLES A LA INGENIERÍA SOCIAL?

Una de las cuestiones que mayor auge tiene en el tema de la Ingeniería Social es sin duda el saber quiénes son el blanco fácil de susceptibilidad para ser víctima de esta efectiva técnica. Seguramente te sorprenderá lo que a continuación se describe:

Es vulnerable de Ingeniería Social *cualquier compañía, sin importar su tamaño*. Si un empleado inconscientemente proporciona información en un correo electrónico o responde a preguntas en una conversación telefónica, permitirá que el intruso actúe desde el interior de la red, sin tener que lanzar ataques desde fuera que rompan las distintas capas de seguridad.

Los ataques de ingeniería social son más efectivos en las grandes empresas pues éstas tienen muchos problemas para manejar sistemas de información con infraestructuras de red complejas, múltiples sucursales y cientos o miles de usuarios. Las políticas y los procedimientos son mucho más difíciles de administrar en este tipo de ambientes y un atacante puede contactar a distintas personas en la organización para ir obteniendo pequeñas piezas de información que le proporcionen un mapa de la misma.

Por el contrario, es más difícil, pero no es imposible, lograr un ataque exitoso de Ingeniería Social en una empresa pequeña, porque normalmente los empleados están en contacto estrecho unos con otros a tal grado que incluso pueden reconocer sus voces en una charla, además de que las políticas y los procedimientos se difunden con mayor efectividad. Sin embargo, *cualquier usuario es vulnerable a ataques de ingeniería social vía correo electrónico, Internet, por teléfono, mensajes de texto (SMS) o sistemas de mensajería instantánea (MSN, Skopie, entre otros).*

La ingeniería social funciona en empresas de todos tamaños pero no existe una fórmula única para que sea exitosa. En organizaciones grandes es difícil detectar un ataque de este tipo pues no hay un método predefinido que un hacker o cracker empleará contra cualquier empresa: lo hará en múltiples capas y niveles jerárquicos, con un alto nivel de creatividad y diseñado para cada caso.

Entidades susceptibles a ataques de ingeniería social

Fig.18. Entidades susceptibles a ataques de Ingeniería Social. Fuente: Elaboración propia.

2.2.1 ¿POR QUÉ EXISTE SUSCEPTIBILIDAD A LOS ATAQUES DE INGENIERÍA SOCIAL?

Las características psicológicas de las víctimas son la razón principal por la que los ataques de Ingeniería Social son exitosos. La gente generalmente se siente a gusto ayudando a otros y evitando las confrontaciones. Tenemos una tendencia natural a confiar en otros, sobre todo en aquellos que tienen un aire de autoridad o de confiabilidad.

Los Ingenieros Sociales típicamente emplean parte de su tiempo en investigar a sus víctimas y buscan de manera sistemática información y terminología que les proporcione credibilidad para parecer miembros de la organización a atacar. Cuando contactan a un empleado pueden emplear frases como: "Estoy llamando del departamento de TI[12] para dar seguimiento a su problema de acceso a la red", que normalmente son muy valiosas sobre todo cuando el atacante ofrece resolver alguna falla.

Es raro que los empleados se den cuenta de la importancia y relevancia de los pequeños trozos individuales de información como lo puede ser el nombre de una persona o un sistema. Los Ingenieros Sociales colectan información de múltiples fuentes para construir con ello un panorama general. Conforme acumulan más datos, aumenta la posibilidad de engañar a otros empleados para que revelen aún más información.

Hay muchos factores que se combinan para que un Ingeniero Social pueda llevar a cabo su labor, pero fundamentalmente emplean en su favor técnicas que explotan las características y debilidades naturales de la gente. Un atacante aprovechará estas debilidades y manipulará a su víctima para que le revele información sensible.

Algunos de los rasgos psicológicos de las víctimas que facilitan el trabajo de los atacantes son los siguientes:

Rasgos psicológicos de las víctimas que facilitan el trabajo de los atacantes

[12] TI: Tecnologías de la Información.

Fig. 19. Rasgos psicológicos que facilitan el trabajo de los atacantes.
Fuente: Elaboración propia.

2.3 ¿POR QUÉ SE USA LA INGENIERÍA SOCIAL?

En una auditoría de hacking ético o un ataque tradicional por medio de métodos y herramientas tecnológicas se pueden necesitar semanas e incluso meses de recopilación pasiva de información antes de intentar romper la seguridad de una red.

El nivel de complejidad de los sistemas de la red también determinará el tiempo de investigación que un atacante necesitará antes de intentar realizar un ataque directo. Además, tendrá que estar familiarizado con la tecnología empleada y deberá tener experiencia para poder vencer las distintas capas de seguridad sin activar alarmas ni dejar evidencia de su paso. Como puede verse se necesita mucho tiempo para investigar, planear y ejecutar un ataque.

Por el contrario, si el cracker o el hacker utilizan métodos de Ingeniería Social efectuarán la misma investigación, pero su objetivo serán los empleados de la organización, con ello estarán evitando los sistemas de seguridad de la red tal como medidas de seguridad lógicas y físicas implementadas en la empresa u organización, y simplemente harán uso de la manipulación hacia los empleados para que revelen información sensible. Esto se realizará con la ayuda de la creación de un escenario y una identidad para después lanzar el ataque. El ingeniero social contactará a la víctima poniendo en práctica diferentes

métodos para manipularla, de manera que sea difícil de detectar su intromisión por personas que no tienen el entrenamiento apropiado en seguridad.

2.4 CLASIFICACIÓN DE LA INGENIERÍA SOCIAL

Debido a su naturaleza, existen dos vertientes que clasifican a la ingeniería Social de acuerdo con el tipo de ataque que se emplee para su uso, estas son: la basada en la tecnología, y la basada en el engaño humano. Ambas trabajan manipulando y engañando al usuario y tienen diferentes niveles de éxito dependiendo de la víctima.

2.4.1 ENGAÑO BASADO EN LA TECNOLOGÍA

En este tipo de Ingeniería Social tanto el hacker como el cracker intentan engañar al usuario mediante la interacción con éste por medio de una aplicación o un sistema que el propio hacker o cracker controla. Algunos ejemplos de ello se enuncian a continuación:

Ejemplos de ingeniería social basada en la tecnología (1a. parte)

Fig. 20. Ejemplos de Ingeniería Social basada en la tecnología (1a. Parte).

Fuente: Elaboración propia con base en *Social Engineering Framework*.

Ejemplos de ingeniería social basada en la tecnología (2a. parte)

Phishing

Éste es un vector de ataque muy conocido que hace pasar un mensaje de correo falso como si fuera legítimo y que normalmente solicita información confidencial como nombres de usuario y contraseñas de un sistema (un portal bancario, por ejemplo). El mensaje por lo general alerta al usuario de alguna consecuencia si no realiza la acción solicitada. El correo llevará al usuario a un sitio falso que se ve igual al sitio legítimo en el que el hacker robará la información deseada.

Pharming

Esta técnica se emplea comúnmente para redireccionar a un usuario de un sitio Web a un sitio falso sin que se dé cuenta mediante algo conocido como "domain spoofing" o suplantación de nombre de dominio.

Vishing

Este ataque es una combinación de Phishing y voz. Por lo regular emplea un sistema interactivo de respuesta (IVR, interactive voice response) falso para recrear el IVR real de una empresa. La víctima es incitada a llamar al IVR falso, vía Phishing o un correo electrónico, para "verificar" cierta información. Finalmente el sistema obtendrá datos como nombres de usuario o contraseña, ya sea de manera automatizada o incluso transfiriendo al usuario con un falso agente de soporte o de atención a usuarios.

Fig. 21. Ejemplos de Ingeniería Social basada en la tecnología (2a. Parte).

Fuente: Elaboración propia con base en *Social Engineering Framework*

2.4.2 ENGAÑO HUMANO

Estas técnicas, difíciles de detectar por una persona no capacitada, emplean debilidades en el comportamiento humano y frecuentemente se basan en la suplantación de personas con cierto nivel de autoridad en la organización:

Fig. 22. Ejemplos de Ingeniería Social basada en el engaño humano.
Fuente: Elaboración propia con base en *Social Engineering Framework.*

De esta manera, por ejemplo, el atacante llamará por teléfono y creará un escenario que convencerá a la víctima de que se trata de alguien confiable. Un típico ataque de este estilo es suplantar a un superior jerárquico que requiere acceso remoto y que ha olvidado su contraseña, por lo que solicita su cambio, pues necesita acceder a cierto sistema de manera urgente. Otros ejemplos del uso de la Ingeniería Social basado en el engaño humano son:

- **Ganar acceso físico:** Un atacante puede suplantar a un empleado de la compañía telefónica para lograr acceso físico a un edificio. Otro ejemplo de este tipo de ataque es la suplantación de un empleado de una empresa de mensajería o de un cliente.

- **Shoulder surfing:** Es una técnica muy empleada y consiste en espiar "sobre el hombro" (de ahí su nombre) a los usuarios cuando teclean su nombre y contraseña en algún sistema.

- **Baiting:** Los atacantes pueden dejar "olvidados" CD, DVD o dispositivos USB con software malicioso, con la esperanza de que los usuarios de una organización los inserten en sus computadoras. Normalmente se dejarán en el estacionamiento o en cualquier lugar cercano a las oficinas de la empresa que se está atacando y pueden incluso contener etiquetas llamativas para incitar su revisión: "Lista anual de bonos" o "Información confidencial".

- **Ingeniería social inversa:** Éste es un método más avanzado que se presenta cuando el atacante crea una persona que parece estar en una posición de autoridad y al cual, a diferencia de otros ataques, los empleados se dirigirán para solicitarle información. Es una técnica muy poderosa pero muy difícil de llevar a cabo pues exige una gran cantidad de recursos y tiempo en la investigación y preparación del ataque. La ingeniería social inversa tiene tres grandes etapas: sabotaje, anuncio y asistencia. Un ejemplo que deja claro estas etapas es el siguiente:

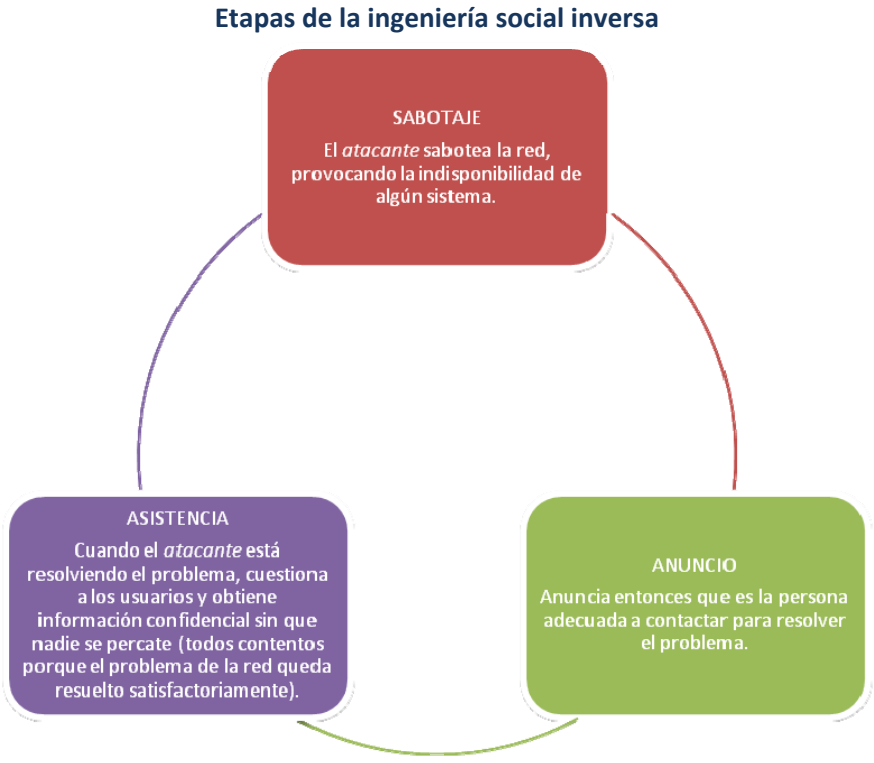


Fig. 23. Etapas de la Ingeniería Social Inversa
Fuente: Elaboración propia.

2.5 CICLO DE ATAQUE DE LA INGENIERÍA SOCIAL

Según la investigación de Gartner, Inc. (NYSE:IT), quien es considerada como el líder mundial en investigación de tecnología de información y consultoría, el ciclo de ataque de la Ingeniería Social consta de 4 etapas, las cuales se describen a continuación:

Fig. 24. Ciclo de ataque de la Ingeniería Social.
Fuente: Elaboración propia con base en *Gartner Research* en http://www.gartner.com/gc/webletter/security/issue1/index.html

2.6 LA INGENIERÍA SOCIAL Y SU RELACIÓN CON LAS REDES SOCIALES

La Ingeniería Social era, y sigue siendo, una de las prácticas más usadas en internet para manipular a una persona y conseguir que haga aquello que nosotros queramos. Según la Ingeniería Social, el primer fallo de seguridad es el aplicado por una persona, esto quiere decir que en ocasiones, es más fácil engañar a una persona para conseguir una contraseña, que intentar conseguirla por otros medios.

Se comenzó con los chats, donde una persona daba su mail para contactar personalmente con otra (anteriormente de Hotmail, Yahoo, Gmail, entre otras) y se entablaba una conversación en donde acababan preguntándole a la víctima la pregunta secreta que se elegía de una lista existente. Por ejemplo, el nombre de mi primera mascota, el nombre de mi primer auto, el nombre de mi primer profesor, etcétera. Acto seguido se conseguía acceso a la cuenta de correo y se cambiaba tanto la contraseña como la pregunta secreta, dejando a esta persona sin correo electrónico, y lo peor de todo, el atacante conseguía toda una lista de contactos a los cuales podría seguir engañando suplantando la identidad de la víctima, o bien distribuyendo virus o spam.

Posteriormente, con las redes sociales, no sólo pueden acceder a nuestra correspondencia, puesto que la gente suele poner la misma contraseña que en su cuenta de correo, sino que además pueden acceder a fotos, videos, intereses y lo más importante, a elementos como fotos, videos e intereses de otras personas ajenas. Esto implica poder llevar a cabo una estafa en línea mucho mayor, ya que se tienen al alcance muchos más datos sobre la vida de una persona y con ello se puede preparar un personaje mucho más creíble. Ejemplo de ello es lo que le pasó a una mujer norteamericana, cuando a una amiga suya le robaron la cuenta. Se hicieron pasar por ella y su novio, pidiendo ayuda solicitando dinero para volver a casa, debido a que supuestamente les habían robado todos sus bienes (maletas, dinero, etcétera) mientras se encontraban de viaje en Londres. Esta mujer, de buena fe, les envió dinero por medio de Western Union, una empresa de envío de dinero donde se pierde el rastro de localización al lugar a dónde se dirige el envío dada su capacidad de anonimato. Cuando la persona legítima de la cuenta se conectó, vio lo ocurrido y avisó a todos sus contactos que alguien se había conectado a su cuenta, y había hecho uso de ella. Demasiado tarde para su otra amiga que ya había enviado dinero a quién sabe quién.

Nunca hay que dar dinero a nadie que lo pide por internet, ya que acceder a una cuenta es, en ocasiones, extremadamente sencillo, ni siquiera tener la confianza de divulgar información a través de las redes sociales a cualquier persona. La gente no elije una buena contraseña, y muchas veces dan pistas de como averiguarlo sin saberlo. O incluso la dejan memorizada en computadoras públicas de bibliotecas, cibercafés, o en la oficina de trabajo.

2.6.1 ¿QUÉ SON Y CÓMO FUNCIONAN LAS REDES SOCIALES?

Imaginemos un grupo de empleados que se reúne en torno a la máquina de café. Bromean, comentan, charlan, discuten. El juego ha comenzado y quien mejor maneje las fichas, con aprendizaje e inteligencia, tendrá el éxito mucho más a mano. Parece una broma, pero no lo es. Las Redes sociales que tejemos en nuestro entorno empresarial, interna y externamente, son miles de veces más útiles que nuestro *currículum vitae*.

Es conocida la anécdota del hombre que consiguió las claves de seguridad de la computadora de un alto directivo sin necesidad de saber absolutamente nada de hacking, cifrados, protocolos y demás. De lo que sí sabía, y mucho, era de rede sociales. Bastaron unas cuantas llamadas, un despliegue absoluto de educación, psicología e inteligencia para que acabaran cediéndoselas.

Como siempre, y mucho más en el mundo en que vivimos, existe mucha información sobre redes sociales, tanto en internet (debido a que es uno de los mejores ejemplos prácticos de lo que puede entenderse como Redes Sociales, pero, no el único) como en revistas de todo tipo. Y se dice de todo tipo porque el concepto de redes sociales es aplicable o abarcable desde distintos y múltiples modelos de relación, y es válido para movimientos sociales, políticos, redes de contactos, amistad, búsqueda de pareja o, incluso, empresas.

El concepto de red social, creado por la antropología inglesa para superar análisis estructurales obsoletos, parte de un abstracto, esto es, se toma un punto de partida de estudio y se establecen las distintas relaciones entre los individuos. Por cada punto de partida se crean distintas redes y por supuesto distintos modelos de relación. Este concepto, tan básico como sencillo es lo que hace de las Redes Sociales un mundo espectacularmente útil y ampliamente difícil de abarcar. Y no solo eso, dentro de un mismo momento o espacio temporal, se pueden redimensionar y redefinir esas Redes Sociales.

Dado el enfoque que se le dará a dicha investigación, un cúmulo de instituciones dentro del sector financiero se construirá el análisis desde dos aspectos fundamentales, la Red Social de una empresa, tanto desde el punto de vista interno como externo, y, por supuesto, desde las posibilidades e imposibilidades de Internet como Red "preconfigurada".

En un artículo de Larissa Adler Lomnitz[13] para REDES, Revista hispana para el análisis de redes sociales, se citan los tres pilares del hombre social:

> En sociedades complejas el individuo debe manejar los tres tipos de intercambio (reciprocidad, redistribución y mercado); ello implica que participa simultáneamente de los tres tipos de relaciones sociales: *una relación de confianza, una de jerarquía y otra de clase*. Así, lo económico, lo político y lo sociocultural son tres dominios que se van enhebrando en la vida del individuo y su trama va conformando la realidad macrosocial (Radcliffe-Brown, 1952, y para la relación entre redes verticales y poder, ver Blau, 1964). Cada tipo de intercambio tiene sus reglas que el individuo aprende a manejar y -cuando son contradictorias- a conciliar entre sí para cada situación determinada. Ese proceso es rico en lenguaje simbólico, por lo tanto la habilidad para manejar símbolos a su vez constituye un recurso. (Lomnitz, 2002).

De lo anteriormente expuesto, cabe resaltar que independientemente de lo acertado o no de la división surgen dos elementos a los que posteriormente se hará referencia y que, en el ámbito empresarial, especialmente, pueden llegar a constituir el éxito o fracaso de una iniciativa, un proyecto o una presentación de producto: el aprendizaje del funcionamiento de las Redes Sociales y la habilidad e inteligencia para manejarlas.

Otro modelo en el que nos podemos fijar, más alejado de conceptos materialistas, lo encontramos ya en Freud, cuando se acerca al concepto de Cultura como herramienta que utiliza el hombre para alejarse de lo animal e impulsivo, desde ahí se retomaría el análisis considerando los conceptos que subyacerían a las

[13] Adler Lomnitz, Larissa (2002). Redes sociales y partidos políticos en Chile. *Revista hispana para el análisis de redes sociales*. 3(2). Recuperado el 2 de octubre de 2011 de la base de datos RedIRIS.

relaciones ahora así consideradas de superación, motivación, interés, manipulación, altruismo, entre otros; y aunque no pudo desligarlo de conceptos marxistas sí se adentró en otros puntos como el de la resignación, muy importante a la hora de considerar las Redes Sociales en una empresa.

Finalmente, y por acercarnos a análisis más cercanos en el tiempo, hay que entender que en el juego de las Redes Sociales hay que contar con tres elementos fundamentales: *los actores, las ideas y las estructuras que generan.* En una empresa, todos somos actores, todos tenemos ideas (propias, corporativas, metodológicas, funcionales) y todos formamos parte de una multiplicidad de estructuras, por mucho que los responsables de encuadrar los departamentos crean tener a todos los empleados "clasificados".

2.6.2 EJEMPLO DE ESTUDIO DE REDES SOCIALES EN UNA ORGANIZACIÓN

Imaginemos a un grupo de personas en nuestra empresa reunidas en torno a una máquina de café. Si iniciamos el estudio considerando las relaciones meramente estructurales de la empresa (dibujaríamos un esquema de vínculos verticales entre los responsables, managers o directivos y sus subordinados. Ya podríamos construir una Red Social posiblemente piramidal en el que el mero comentario del tema salarial se obviaría, pues no cabe que hablemos del salario junto a la máquina de café frente a quienes lo han de decidir.

Sin embargo, si se toma como elemento de estudio, por ejemplo, el ámbito personal, estableceríamos una Red Social donde las relaciones se verían desordenadas por aquellos cuya personalidad es extrovertida, con comportamiento de liderazgo, frente a los más tímidos o refugiados en sus problemas de aceptación. Se podría ahora dibujar una Red Social circular donde el centro lo ocuparía aquella o aquellas personas que dirigen la conversación, que son el centro de atención de los demás, ya sea por fascinación, por humor, por simpatía, por empatía, etcétera.

Finalmente, y para no olvidarnos de uno de los modelos más estudiados y que más negocio está creando en la red, podríamos acercarnos al grupo desde sus relaciones sentimentales o sexuales. Entonces la Red Social estaría complejamente tejida entre, por ejemplo, los solteros, los casados, los divorciados, naturalmente entre heterosexuales y homosexuales, creándose nuevos vínculos, con una estructura horizontal realmente complicada donde lo que primaría sería el interés, los sentimientos, las historias personales, entre otras.

Es por tanto necesario que se establezca ,antes de analizar una Red Social, un punto de partida o modelo de relación social para poder acercarnos con algunas posibilidades de éxito, cuestión nada fácil, dado el cúmulo de información a la que estamos sometidos, así como a las herramientas de comunicación que nos abruman cada vez más en la sociedad actual. Sin embargo, esto no es imposible y siempre se crea un escenario distinto y adecuado para cada situación.

Ejemplo de estructura de redes sociales

Fig. 25. Ejemplo de Estructura de Redes Sociales

2.6.3 CRECIMIENTO DE LA INGENIERÍA SOCIAL EN LAS REDES SOCIALES

La idea de trasladar nuestra realidad al campo virtual es la máxima del momento. Progresivamente vamos adaptando nuestra vida cotidiana a las comodidades que se nos ofrecen y están a nuestro alcance. Probablemente para aquéllos que trabajen constantemente, se les complique el tener una vida social activa. "El tiempo es oro". Vivimos bajo las reglas capitalistas que desencadenan una modificación constante sobre la cultura y la sociedad.

De la misma forma que la gente que se conoce de manera personal o virtual se cae en una simple inconsistencia dentro los niveles de verdad entre la información real y la información virtual, por transitividad se induce a que sería mucho más fácil que alguien que no conociéramos fuera manipulado a través de la modificación o la creación de información "falsa", la cual sería imposible de ser constatada por dicha persona. Este punto es cúspide en esta investigación, ya que recordemos que los atacantes hacen uso de esta técnica brindando información falsa que no es constatada por los terceros en discordia.

Sin embargo, cabe recalcar que la información divulgada en las redes sociales actuales, tales como *Facebook, Hi5, Twitter, Linkedin*, etcétera, son un cúmulo de información importante que si bien, las personas no lo emplean de manera adecuada implementan la configuración de restricciones correspondientes, puede ser un nicho interesante y susceptible de explotar por para el atacante, para crear posibles escenarios que favorezcan su intervención en un ataque de ligas mayores como por ejemplo en las empresas u organizaciones.

Es por ello, que me gustaría concluir este apartado exponiendo que las Redes Sociales no son malas, simplemente debemos saber utilizarlas de manera adecuada restringiendo los permisos correspondientes, Así mismo, se debe ser cuidadoso de la información que se comparte, ya que, el mal uso de dicha información puede propiciar un vínculo que funciones como el eslabón de una larga cadena que empleará el atacante con fines maliciosos y en contra de la empresa en la que laboramos, o peor aún, hacia nosotros mismos.

Algunos ejemplos de redes sociales en la web

Fig. 26. Algunos ejemplos de Redes Sociales en la Web.

2.7 ESTUDIOS REALIZADOS

ESTUDIO 1

Se realizó un estudio al que se le dio el nombre de "Ingeniería Social: Psicología aplicada a la seguridad informática", el cual fue realizado por el alumno Sergio Arcos Sebastián y publicado el 1 de junio de 2011 en Barcelona España.

El proyecto toma los fundamentos de los ataques de ingeniería social en los sistemas informáticos, especialmente en las grandes plataformas de Internet. El objetivo principal es lograr comprender su naturaleza y ser capaces de valorarlos como la amenaza que representan.

Con la finalidad de conseguir el objetivo se realizaron pruebas de concepto para valorar el riesgo, cambiando a menudo la perspectiva a la del atacante. A raíz de este proyecto, se espera formar una base, para que en un futuro sea posible incrementar la seguridad de dichas plataformas con tecnologías de prevención, detección e intercepción de estos ataques, proponiendo la "Interacción Humano-Computadora Segura" como punto de partida.

El lector, aun no siendo responsable del mal diseño de las plataformas de Internet ni culpable de la pérdida de sus propios datos, puede concienciarse con los ejemplos mencionados y reaccionar más sabiamente en futuras situaciones delicadas.

El instrumento que se empleó fue el desarrollo de una página Web en la cual se cuestiona al lector para que responda a ciertas preguntas relacionadas con la ingeniería social, sin que este lo sepa directamente, así mismo, se realiza la recaudación de los datos proporcionados durante la aplicación del instrumento.

FICHA TÉCNICA

ESTUDIO REALIZADO 1			
Autor(es):	Sergio Arcos Sebastián		
Características del Estudio			
Nombre:	Ingeniería social: Psicología aplicada a la seguridad informática		
País:	Barcelona, España	**Fecha:**	01 de junio de 2011
Descripción del estudio:			

El proyecto toma los fundamentos de los ataques de ingeniería social en los sistemas informáticos, especialmente en las grandes plataformas de Internet. El objetivo principal es lograr comprender su naturaleza y ser capaces de valorarlos como la amenaza que representan.

Con la finalidad de conseguir el objetivo, se realizaron pruebas de concepto para valorar el riesgo, cambiando a menudo la perspectiva a la del atacante. A raíz de este proyecto, se espera formar una base para que en un futuro sea posible incrementar la seguridad de dichas plataformas con tecnologías de prevención, detección e intercepción de estos ataques, proponiendo la "Interacción Humano-Computadora Segura" como punto de partida.

El lector, aun no siendo responsable del mal diseño de las plataformas de Internet ni culpable de la pérdida de sus propios datos, puede concienciarse con los ejemplos mencionados y reaccionar más sabiamente en futuras situaciones delicadas.

Instrumento(s) empleado(s):	Página Web

Descripción del instrumento:

El instrumento empleado para dicha investigación fue la elaboración de una página web para vaciado de datos, haciendo uso de una base de datos en donde se guardaban los datos correspondientes.

Ver Anexo 1

ESTUDIO 2

Se desarrolló un kit de herramientas de Ingeniería Social denominado "Social Engineering Toolkit 1.0" , herramienta que fue desarrollada por Dave Kennedy (ReL1K), un ex marine de los Estados Unidos y actual director de seguridad de una compañía incluida en la lista de "Fortune 1000".

Este Kit, conocido como *SET (Social Engineers Toolkit)* y que ha sido descargado más de 1. Millones de veces de la red, es una herramienta poderosa que se puede emplear para ataques de ingeniería social. Se trata de un script[14] desarrollado en el lenguaje de programación *Python* que se integra con el marco de referencia del famoso Metasploit[15] (Compendio de herramientas que permiten explotar vulnerabilidades en un

[14] En informática, un script o como también se le conoce, un archivo de órdenes o archivo de procesamiento por lotes, es un programa simple, que se almacena en un archivo de texto plano y cuyo uso fundamental resulta a la hora de tener que realizar diversas tareas como ser la combinación de componentes, la interacción con el usuario o con el sistema operativo en cuestión.

[15] Open Source Community and Rapid7 (2012). Metasploit. USA. Recuperado el 29 de abril de 2012 en http://www.metasploit.com

sistema) y que permite el desarrollo de ataques de *Pshising* basados en correo y en Web de una manera muy sencilla mediante una interface de línea de comandos.

El software tiene varios vectores de ataque que se usan para explotar las vulnerabilidades de un sistema y puede combinarse con técnicas de engaño humano para ganarse la confianza de la víctima. Algunos ejemplos de vectores de ataque son los siguientes:

- Spear-phising
- Web site
- Generador de medios infecciosos (para crear ejecutables y archivos autorun.inf que crean una sesión entre la víctima y el atacante)
- Generador de correos en masa
- Teensy USB HID
- SMS Spoofing

Para mayores detalles sobre este kit, consulte la página Web http://www.social-engineering.org/se-resources/

FICHA TÉCNICA

ESTUDIO REALIZADO 2			
Autor(es):	Dave Kennedy		
Características del Estudio			
Nombre:	*Social Engineering Toolkit* 1.0 - 1.1 SET		
País:	Estados Unidos	**Fecha:**	Aproximadamente 2010
Descripción del estudio:			
The Social-Engineer Toolkit mas conocido como SET es un conjunto de herramientas especialmente diseñadas para realizar ataques de Ingeniería Social en procesos de auditorías en seguridad, está programado en Python por David Kennedy (ReL1K), quien hace poco publicó su versión 1.1 con grandes cambios.			
Instrumento(s) empleado(s):	Herramienta para desarrollar ataques de Ingeniería Social		

Descripción del instrumento:
Al iniciar el SET, lo primero que vemos es un menú que nos ofrece una gran cantidad de opciones para lanzar nuestro ataque de ingeniería social, desde la creación de correos fraudulentos, paginas que al visitarlas infecta tu maquina, archivos multimedia que permite obtener acceso al equipo de la víctima, la posibilidad de enviar correo masivo, crear un CD/DVD o memoria USB que infecte la maquina y hasta enviar mensajes de texto que nos ayude en nuestra tarea. Ver anexo 2

ESTUDIO 3

Dicho caso de estudió se denominó “Espionaje Industrial a través de la ingeniería social” realizado por Ira S. Winkler de la National Computer Security Association en Estados Unidos sobre los ataques actuales de espionaje industrial en contra de una gran corporación de U.S

El estudio de caso para dicha presentación direcciona a la realización de una prueba de penetración efectuada a una empresa de alta tecnología en respuesta a su petición. El objetivo de la prueba fue para simular un ataque de espionaje industrial, dentro de los parámetros de financiación. Una estrategia de ataque global fue utilizada para simular un ataque de la mayor precisión posible. El ataque incluyó el uso de la investigación de código abierto, la obtención de un puesto como empleado temporal en el objetivo, la tergiversación de las responsabilidades del empleado temporal, abuso de acceso físico, la piratería informática interna, la coordinación interna y la facilitación de hackers externos, y el hacking externo derecho.

Los resultados fueron asombrosos. En un lapso de un día en las actividades del lugar más de $1,000,000,000 de dólares de la información fue "robada". Mientras que el firewall era impenetrable y las tarjetas inteligentes impedían el acceso de extraños, la información fue comprometida casi a voluntad por un allegado (empleado de la compañía). Esto se logró en una empresa que tiene un tremendo programa de seguridad técnica. El administrador de seguridad comprende sus vulnerabilidades, y quería una evaluación independiente de las vulnerabilidades para demostrar la seriedad del problema.

FICHA TÉCNICA

ESTUDIO REALIZADO 3	
Autor(es):	Ira S. Winkler de la *National Computer Security Association*

Características del Estudio			
Nombre:	Caso de Estudio de Espionaje Industrial a través de la Ingeniería Social		
País:	Estados Unidos	**Fecha:**	13 de septiembre de 1996
Descripción del estudio:			
El objetivo de la prueba fue para simular un ataque de espionaje industrial, dentro de los parámetros de financiación. Una estrategia de ataque global fue utilizada para simular un ataque de la mayor precisión posible. El ataque incluyó el uso de la investigación de código abierto, la obtención de un puesto como empleado temporal en el objetivo, la tergiversación de las responsabilidades del empleado temporal, abuso de acceso físico, la piratería informática interna, la coordinación interna y la facilitación de hackers externos y el hacking externo derecho.			
Instrumento(s) empleado(s):	Prueba de penetración (*pentest*)		
Descripción del instrumento:			
Se efectuaron las pruebas de penetración pertinentes haciendo énfasis en la aplicación de la técnica de la ingeniería social, incluyendo un espía en la empresa el cual ocupó un puesto temporal en la empresa para poder obtener información, investigación de código abierto, la tergiversación de las responsabilidades del empleado temporal, abuso de acceso físico, la piratería informática interna, la coordinación interna y la facilitación de hackers externos, y el hacking externo derecho.			

ESTUDIO 4

Dicho estudió recibió el nombre de "Ingeniería Social: Explotando la debilidad humana" y fue desarrollado en la India por Wasim "washal" Halani un integrante de la empresa Network Intelligence India Consulting (NIIConsulting) en junio del 2010.

Para dicho estudio se emplearon herramientas y técnicas de ataque tales como:

- Phishing
- Bainting
- Robo de Identidad
- Chequeo en el basurero
- Email Scams

- Uso de autoridad
- Petición de ayuda
- Caer en la curiosidad
- Abuso de confianza

Dicho estudio se realizó en una compañía de Tecnologías de la Información, la cual contaba con 2 oficinas y un número aproximado de 400 a 500 empleados. NIIConsulting había realizado previamente otros proyectos de seguridad en dicha organización, los guardias estaban familiarizados con los integrantes que aplicaron el estudio y cabe destacar que se conocía a algunas personas de sus proyectos previos. Sólo tres personas de la organización estuvieron conscientes de lo que se realizaría y se procedió a l aplicación del mismo.

La finalidad de dicho estudio era demostrar que la ingeniería social es una técnico poderosa con la cual se puede obtener información de la cadena más débil "el ser humano".

FICHA TÉCNICA

ESTUDIO REALIZADO 4			
Autor(es):	Wasim "washal" Halani		
Características del Estudio			
Nombre:	Ingeniería Social: Explotando la debilidad humana		
País:	India	**Fecha:**	09 de junio de 2010
Descripción del estudio:			
Dicho estudio se realizó en una compañía de Tecnologías de la Información, la cual contaba con 2 oficinas y un número aproximado de 400 a 500 empleados. NIIConsulting había realizado previamente otros proyectos de seguridad en dicha organización, los guardias estaban familiarizados con los integrantes que aplicaron el estudio y cabe destacar que se conocía a algunas personas de sus proyectos previos. Sólo tres personas de la organización estuvieron conscientes de lo que se realizaría y se procedió a l aplicación del mismo. La finalidad de dicho estudio era demostrar que la ingeniería social es una técnico poderosa con la cual se puede obtener información de la cadena más débil "el ser humano".			
Instrumento(s) empleado(s):	Se emplearon una serie de herramientas y técnicas las cuales se		

	enuncian en el siguiente rubro
Descripción del instrumento:	
• Phishing • Bainting • Robo de Identidad • Chequeo en el basurero • Email Scams • Uso de autoridad • Petición de ayuda • Caer en la curiosidad • Abuso de confianza Ver anexo 3	

ESTUDIO 5

Dicho estudió fue publicado en el *Proceedings of the Fifth USENIX UNIX Security Symposium* por Ira S. Winkler y Brian Dealy en el estado de Utah USA. Dicho estudio recibió el nombre de "¿Tecnologías de la Información de Seguridad? ... No confiar en ella. Un caso de estudio en la ingeniería social – "Information Security Technology?...Don't Rely on It A Case Study in Social Engineering" realizado en junio de 1995.

El caso de estudio que se describe no representa una sola operación. Para proteger a los clientes de los autores, el estudio de representa una compilación de varios ataques reales contra las grandes instituciones financieras. Estos ataques se llevaron a cabo como parte de un análisis de vulnerabilidades integral para las organizaciones. Mientras que los funcionarios de la empresa eran conscientes de un posible ataque, el resto de los empleados de las empresas no lo eran. Todo lo descrito en el caso de estudio ha ocurrido en múltiples ocasiones.

Los "atacantes" se limitan a la recopilación de información por teléfono, y se instruyó específicamente a no explotar el sistema con la información. El ataque fue limitado a cuatro días-hombre de esfuerzo, lo que requirió que los atacantes fueran más "audaces" de lo que se requiere normalmente. Un verdadero ataque de ingeniería social se llevaría a cabo durante semanas, incluso meses. Un ataque real podría haber incluido varias visitas físicas a las oficinas de la empresa y, posiblemente, incluso la obtención de un puesto de trabajo en la empresa.

Dicho estudio fue realizado empleando:

- La combinación de datos de un reporte anual con los datos obtenidos de internet efectuando con ello una lista de nombres y puestos ocupados en la organización.
- Uso del teléfono de la empresa que redirecciona a áreas especificas las llamadas.

- Uso del directorio telefónico.
- Obtención de sistemas operativos empleados al hacer uso de una máquina, así como las aplicaciones en uso ID y password.

FICHA TÉCNICA

ESTUDIO REALIZADO 5			
Autor(es):	Ira S. Winkler y Brian Dealy		
Características del Estudio			
Nombre:	Tecnologías de la Información de Seguridad? ... No confiar en ella Un caso de estudio en la ingeniería social – "Information Security Technology?...Don't Rely on It A Case Study in Social Engineering"		
País:	Utah, Estados Unidos	**Fecha:**	junio de 1995
Descripción del estudio:			
El caso de estudio que se describe no representa una sola operación. Para proteger a los clientes de los autores, el estudio representa una compilación de varios ataques reales contra las grandes instituciones financieras. Estos ataques se llevaron a cabo como parte de un análisis de vulnerabilidades integral para las organizaciones. Mientras que los funcionarios de la empresa eran conscientes de un posible ataque, el resto de los empleados de las empresas no lo eran. Todo lo descrito en el caso de estudio ha ocurrido en múltiples ocasiones.			
Instrumento(s) empleado(s):	Se emplearon una serie de herramientas y técnicas las cuales se enuncian en el siguiente rubro		
Descripción del instrumento:			
Dicho estudio fue realizado empleando: • La combinación de datos de un reporte anual con los datos obtenidos de internet efectuando con ello una lista de nombres y puestos ocupados en la organización. • Uso del teléfono de la empresa que redirecciona a áreas específicas las llamadas • Uso del directorio telefónico.			

- Obtención de sistemas operativos empleados al hacer uso de una máquina, así como las aplicaciones en uso ID y password.

ESTUDIO 6

Dicho estudio se efectuó en junio del 2010 y recibió el nombre de "Caso de Estudio en Ingeniería Social. Técnicas para la persuasión" – "Case Study on Social Engineering Techniques for Persuasion" el cual fue efectuado por Mosin Hasan, Nilesh Prajapati y Safvan Vohara en la ciudad de Nagar, India.

Partiendo de la primicia de que la ingeniería social es el ataque más poderoso, dichos investigadores trataron de comprobar la eficacia de la ingeniería social en el sistema operativo Linux. Linux es considerado como el sistema operativo más seguro, pero como se ha señalado con anterioridad, aún el sistema más seguro se puede romper por el eslabón más débil (las personas). Dicho caso de estudio muestra el impacto de la Ingeniería Social al conectarla con un Spyware.[16]

FICHA TÉCNICA

ESTUDIO REALIZADO 6			
Autor(es):	Mosin Hasan, Nilesh Prajapati y Safvan Vohara		
Características del Estudio			
Nombre:	Caso de Estudio en Ingeniería Social. Técnicas para la persuasion - *Case Study on Social Engineering Techniques for Persuasion*		
País:	Nagar, India	**Fecha:**	junio de 2010
Descripción del estudio:			
Se creó un spyware para Linux que registra la información tecleada por el usuario en ambientes Linux. No colocaron el spyware con la finalidad de atacar en entorno real, sino para obtener estadísticas relacionadas con Spyware empleando las tácticas de ingeniería social, tratando de lograrlo por medio de tres maneras y			

[16] Spyware: El spyware es un software que recopila información de una computadora (PC) y después transmite esta información a una entidad externa sin el conocimiento o el consentimiento del propietario de la computadora.

todas estas técnicas se basan en la ingeniería social.

Instrumento(s) empleado(s):	1. El entusiasmo de la diversión 2. El afán de saber gran cosa 3. Hoaxing

Descripción del instrumento:

1. El entusiasmo de la diversión: En cuanto a este ataque, primero reunieron la información como si conocieran a la persona en cuestión. Se reunió la información tal como si utiliza el sistema operativo como Linux. Él es aficionado a la programación de scripts en shell de Linux. La segunda etapa fue el desarrollo de una amistad que ya se ha establecido con la persona que elegimos que confíe en nosotros. Lo enviamos a un amigo que usa Linux como sistema operativo de escritorio en el correo. La línea de asunto del correo era “Shell Script for Fun”.

   Como se observa frecuentemente que usuario al recibir un correo electrónico que proviene de un amigo, se esperó que lo abriera, ya que pretende ser de un amigo seguro. Te quedas atrapado, porque incluso se puede enviar correo con un nombre falso que tenga abierta la retransmisión de correo SMTP. Esta es la estrategia psicológica y que se adapta al ataque, una vez que se ha elegido a la persona.

2. El afán de saber gran cosa: El segundo caso se realizó con el mismo principio primordial de la recopilación de información, establecimiento de relación y luego el engaño. Se eligieron las personas aficionadas a la actividad del hacking y cracking informático. Incluso en internet, si se realiza una búsqueda de herramientas libres para el hacking y cracking, seguro que se van a obtener de forma gratuita.

   Sin embargo, muchos de estos programas informáticos hackean tu sistema. En internet: Se puso un enlace a un shell script con el nombre de "Herramienta para hackear Windows" a un amigo. Y al hace clic en éste, los descargó y corrió en su máquina.

3. Hoaxing: como la gente piensa, Linux es más seguro que Windows, pero no saben en qué porcentaje y los usuarios quieren información sobre este aspecto. Así que se realizó un reporte falso de Linux que contenía un Shell Script cómo el caso anterior. Se envió a un amigo como una noticia de nombre: “Informe de seguridad de Linux”. Esperando que la gente normalmente sigua el enlace. Como todas estas técnicas utilizan la ingeniería social, el humano queda atrapado.

Cabe destacar que el spyware requiere privilegios de administrador.

Para ver los resultados del estudio Ver anexo 4

ESTUDIO 7

Existen otros casos de estudio realizados por los investigadores de Ingeniería Social más importantes como son: Marcus Nohlberg, Markus Huber, Daniel Siegel y Kevin Mitnick (2002) quien aborda la técnica de la ingeniería social por medio de un libro. El tema que aborda dicho libro es precisamente el arte del engaño, se trata de ganar la confianza de alguien mintiéndoles y luego abusar de esa confianza para la diversión y el beneficio. Los hackers utilizan el eufemismo de "ingeniería social" y el hacker gurú Kevin Mitnick examina muchos escenarios de ejemplo.

MATRÍZ DE ESTUDIOS REALIZADOS

Nombre de estudio	País	Fecha	Instrumento utilizado	Descripción del instrumento	Indicadores
Ingeniería social: Psicología aplicada a la seguridad informática	Barcelona, España	1 de junio de 2011	Página Web en la cual se cuestiona al lector para que responda a ciertas preguntas relacionadas con la ingeniería social, sin que éste lo sepa directamente,	Pruebas de concepto para valorar el riesgo, cambiando la perspectiva a la del atacante.	- Foto de perfil - Relación - Amistades - Familia - Datos Personales - Previsualización de fotos - Relación tu y yo - Página Muro - Página información - Página imágenes - Página canciones - Pagina amigos
Social Engineering Toolkit 1.0 -1.1 SET	Estados Unidos	Aproximadamente 2010	Herramienta para desarrollar ataques de ingeniería Social	Script desarrollado en lenguaje de programación Python que se integra con el marco de referencia de Metasploit.	Vectores de ataque - Spear Phising - Web site - Creación de ejecutables - Generador de correos en masa - Teensy USB HID - SMS Spoofing
Caso de Estudio de Espionaje Industrial a través de la Ingeniería Social	Estados Unidos	13 de septiembre de 1996	Auditoría de Pruebas de penetración	Se efectuaron las pruebas de penetración pertinentes haciendo énfasis en la aplicación de la técnica de la ingeniería social.	- Espía que ocupó puesto temporal ión - Investigación de código abierto - Tergiversación de las responsabilidades del empleado. - Abuso de acceso físico - Hacking interno - Facilitación de Hacking externo
Ingeniería Social: Explotando la	India	9 de junio de 2010	Uso de herramientas, técnicas y abuso de	Se hizo uso primordialmente del abuso de confianza debido a que se habían	- Phising - Baiting - Robo de Identidad

debilidad humana			confianza	realizado otros proyectos en dicha organización, lo que permitió que ya estuviesen familiarizados con las personas externas y les permitieran el acceso.	- Verificación de información en el cesto de basura - Email Scams - Uso de autoridad - Petición de ayuda - Caer en la curiosidad - Abuso de confianza
Tecnologías de la Información de Seguridad? …No confiar en ella. Un caos de estudio en la Ingeniería Social – "Information Security Technology? … Don´t Rely on It A Case Study in Social Engineering"	Utah, Estados Unidos	Junio de 1995	Ataques reales contra grandes instituciones financieras	Análisis de vulnerabilidades integral para las organizaciones	- Combinación de datos de un reporte anual con los datos obtenidos de internet efectuando con ello una lista de nombres y puestos en la organización. - Uso del teléfono de la empresa que direcciona a áreas específicas - Uso de directorio telefónico - Características y aplicaciones contenidas en los equipos. - Contraseñas y usuarios.
Caso de Estudio en Ingeniería Social. Técnicas para la persuasion-"Case Study on Social Engineering Techniques for Persuasion"	Nagar, India	Junio de 2010	Spyware para Linux que registra la información tecleada por el usuario en ambientes Linux	Se hacía el envío por medio de correo electrónico en donde se ponía como contenido la dirección url del spyware	- El entusiasmo de la diversión - El afán de saber gran cosa - Hoaxing - Correr con privilegios de usuario privilegiado - Correr con privilegios de administrador - No siguieron el link

2.8 ESTADO DEL ARTE

Este proyecto de investigación permite reflexionar respecto al impacto que tiene la ingeniería social en el hacking ético dentro del sector financiero, así como la importancia que tiene una concientización referente a la seguridad de la información debido a que la mayoría de los empleados que integran el corporativo de las empresas no cuentan con una cultura organizativa que conlleve a la cultura de seguridad de la información debida, lo que permite que exista un innumerable índice de fraudes tanto físicos como electrónicos.

Cabe destacar que han existido ávidos e importantes investigadores de la ingeniería Social tales como Kevin Mitnick, Marcus Nohlberg, Markus Huber, Daniel Siegel, y otros. Recopilando el estado del arte que ha realizado cada uno de ellos es posible obtener una visión mucho más precisa, pero dada la rápida evolución tecnológica que ha habido durante los últimos años, todo lo anterior al trabajo de Kevin Mitnick en 2002 está prácticamente obsoleto; sin embargo, cabe aclara que algunos estudios pueden servir de ayuda para comprender a detalle algunas metodologías que aplican la técnica de la Ingeniería Social.

Se ha encontrado que la mayoría de los trabajos efectuados señalados en la matriz de estudios realizados se han ejecutado con mayor auge en paíeses anglosajones como Estados Unidos, seguido de ciudades Indues como Nagar y finalmente en países europeos como España. Dichas investigaciones se han estudiado a partir de los años noventas teniendo gran auge en los últimos años (2010 y 2011), exponiendo metodologías para aplicar la técnica de la Ingeniería Social haciendo uso de medios informáticos y valiéndose de internet empleando el uso de las redes sociales como medio principal para poder aprovecharse del individuo y así extraerle, de sus repositorios digitales, información confidencial y relevante para él, e incluso, en el peor de los casos, se logra extraer la información elemental y de índole confidencial de las empresas en las que labora dicho individuo.

Los instrumentos utilizados, de acuerdo con la matriz de estudios, en su mayoría son diversos, pero convergen en un patrón de uso constante, *el uso de herramientas técnicas y abuso de confianza para desarrollar ataques de Ingeniería Social.* Dichos instrumentos han sido validados con la entrega de resultados a las instituciones en cuestión en lo que concierne a los casos de estudio; y, como herramientas probadas y puestas en marcha por profesionales de la seguridad al hacer uso de las mismas. Asimismo, cabe señalar que los indicadores son diversos, recayendo en variables de tipo dicotómicas, tricotómicas, múltiples, cerradas y abiertas. Dichas variables miden en su mayoría el riesgo ante el cual se encuentran susceptibles los individuos al ser víctimas de la Ingeniería Social. Finalmente, cabe señalar que la Ingeniería Social no es exclusiva de la seguridad informática, se utiliza en todas aquellas disciplinas que tienen un impacto sobre otras personas, consiguiendo ser más eficaces con sus propósitos tal como: la religión, el marketing, la política, entre otros.

En este capítulo hemos abarcado lo referente a la Ingeniería Social como una vertiente del Hacking Ético, ahora veremos cómo estableceremos ese vínculo con el sector financiero.

III. EMPRESAS DENTRO DEL SECTOR FINANCIERO

Hoy en día el sector financiero se encuentra al borde de infinidad de delitos por fraudes debidos a la inmensurable fuga de información proveniente de su organización que los empleados que laboran en la misma muy posiblemente divulgan sin saberlo. El punto medular de este estudio se encuentra en el saber si el nivel de seguridad de la información con el que cuenta un cúmulo de empresas dentro del sector financiero es susceptible de ataque, para posteriormente hacerles del conocimiento de dichas empresas los resultados obtenidos y que se tomen las medidas pertinentes para la mitigación o la merma de dicho riesgo.

Es por ello que se considera importante establecer la caracterización del sector para poder obtener resultado representativos, y, con base en ellos, poder aplicar estrategias, tendencias y tácticas para evitar la fuga de información valiosa para las entidades bancarias.

3.1 ANTECEDENTES DEL SECTOR FINANCIERO

Existen muchas formas de enfrentar los problemas de seguridad actuales. Ciertamente se ha demostrado que la más acertada es conocer la mentalidad del hacking, o en otras palabras, cómo un hacker piensa, actúa y qué técnicas y metodologías utiliza para tomar ventaja de las vulnerabilidades actuales. Es por ello, que surge el hacking ético, una técnica empleada para pensar como hackers y ejecutar una serie de pruebas que permitan verificar la existencia de vulnerabilidades localizadas en los sistemas y demás ámbitos de la empresa, todo ello con la finalidad de mermarlos y disminuir en consecuencia la posibilidad de riegos que la organización pueda presentar, fundamentalmente de la información con la que ésta cuenta.

En adición a lo anteriormente expuesto, se ha detectado a través de los últimos años un crecimiento relevante en cuanto a la tecnología de nuestro país, pero aunado a ello se ha dado auge a un bajo porcentaje de aceptación principalmente por miedo a ser víctimas de fraudes, conllevando a implementar medidas drásticas como el bloqueo de unidades de almacenamiento, prohibición del uso de internet, entre otras; pero, ¿acaso se tendrá una mejora al evitar el uso de herramientas que permiten realizar nuestras labores de manera eficiente? La respuesta es muy simple: por muy robustas que sean las medidas implementadas para la protección de la organización, siempre existirá un factor que de no contar con una ética, cultura y concientización adecuada referente a la seguridad de la información, atentará contra la seguridad de la información y por consiguiente de la misma organización, este factor es el elemento humano.

Si bien es cierto que nunca se podrá tener un entorno seguro al cien por ciento, también es verdad que la probabilidad de riesgo a ser susceptible ante una amenaza puede decrementarse y tender a mejorar, todo depende del ser humano que maneje la información, debido a que el eslabón más débil somos todos nosotros, la primera defensa somos nosotros como entes individuales y es nuestra responsabilidad contribuir para favorecer el fortalecimiento de la seguridad de la información y ética de las organizaciones fomentando una cultura a favor de la protección de la información y de las medidas que se deben emplear para asegurar su confidencialidad, integridad y disponibilidad. Pero, ¿existe alguna técnica que permita verificar que la difusión de la seguridad de la información es la adecuada? ¿Qué es lo que hace que se piense que somos capaces de propagar información confidencial sin proponérnoslo?

La respuesta al primer cuestionamiento es sí existe una técnica que permite la obtención de información sin que la persona que la proporciona lo haga de manera intencional; ésta es la llamada Ingeniería Social. Por otro lado, la segunda respuesta está contenida en investigaciones realizadas por famosos hackers, tal como el muy reconocido en los Estados Unidos, Kevin Mitnick,[17] quien considera que todos los seres humanos somos susceptibles de fracasar con facilidad en este aspecto, ya que los ataques de ingeniería social, muchas veces llevados a cabo por medio de un teléfono o en nuestras conversaciones cotidianas, son basados en cuatro principios básicos y comunes a todas las personas, éstos son: que todos queremos ayudar, que el primer movimiento es siempre de confianza hacia el otro, que no nos gusta decir "no" y el que a todos nos gusta que nos alaguen.

Asimismo, cabe destacar que sus investigaciones y la práctica de las mismas fueron publicadas en su libro *Controlling the Human Element of Security. The Art Of Deception*. Por otra parte, es relevante hacer mención que hoy en día existe una carrera relacionada con ésta habilidosa técnica en el país Sudamericano de Paraguay cuya Universidad Columbia de Paraguay, implementó una propuesta de plan de estudios en 2009 y en marzo del 2010 lo llevó a la práctica refiriéndose a las metodologías empleadas para la ejecución de dicha técnica; sin embargo, actualmente dicho plan de estudios ya no está vigente. De igual manera, en México no se ha tenido registro alguno de investigaciones referentes a dicho tema, sin embargo, se prevé que un futuro lo halla.

Aunado a este tema, tenemos el lugar en donde frecuentemente se suscitan las fugas de información y es precisamente en las empresas que se definen como: "Una unidad económica de producción y decisión que, mediante la organización y coordinación de una serie de factores (capital y trabajo), persigue obtener un beneficio produciendo y comercializando productos o prestando servicios en el mercado" (Andersen, 1999, citado por Zorrilla, 2004),[18] empresas que se abocan al sector financiero y en donde en los últimos años se han presentado numerosos fraudes que han llevado a grandes pérdidas monetarias, además de que el presupuesto y número de trabajadores es variable y por lo mismo dichas organizaciones se preocupan mayoritariamente por la productividad que por la seguridad misma de la organización. Es por ello que el marco de referencia del presente trabajo se limita a las empresas del sector financiero, hecho por el cual me parece pertinente aclarar lo siguiente:

El sistema financiero mexicano, está integrado por:

[17] Mitnick, Kevin. (2002). *Controlling the Human Element of Security. The Art Of Deception*. USA: .John Wiley & Sons Australia.

[18] Zorrilla, Juan P. (2004). La importancia de las pymes en México y para el mundo. GestioPolis. Recuperado el 29 de abril de 2012 en http://www.gestiopolis.com/canales2/economia/pymmex.htm

Instituciones del sistema bancario mexicano

FIg. 27. Instituciones del Sistema Bancario Mexicano.
Fuente: Elaboración Propia con base en la CNBV.

Para fines de este estudio me abocaré a las instituciones de banca Múltiple y de Banca de Desarrollo. La Banca de Desarrollo está integrada por las instituciones encargadas de realizar la intermediación financiera con fines de fomento.

Por otro lado, la Banca Múltiple o Comercial es aquélla que está integrada por todas las instituciones encargadas de realizar la intermediación financiera con fines de rentabilidad, ésta última constituye el centro de la actividad financiera. Capta los recursos del público, sobre los que se constituye su capacidad de financiamiento y haciendo uso de ésta, principalmente en operaciones activas "créditos", realiza su función de promover la creación y desarrollo de las empresas como complemento en la inversión de las sociedades industriales, comerciales y de servicios.

Es principalmente en dichas entidades en donde se presenta un mayor número de fraudes de distinta índole, pero mayoritariamente de tipo informáticos, los cuales traen como consecuencia grandes perjuicios, no solo para los clientes, sino para la propia empresa y por consiguiente para la economía del país. Es por ello, que la unidad de análisis que dicho trabajo tomará en consideración, de acuerdo con el padrón de identidades de Banca Múltiple y de Banca de Desarrollo Supervisadas por la Comisión Nacional Bancaria y de Valores (CNBV), y debido a que es la muestra que marca un mayor tendencia en el estudio, dicha investigación se centra en las siguientes instituciones:

Unidad de análisis (1ª parte)

Fig. 28. Unidad de Análisis (1ª parte).

Fuente: Elaboración Propia.

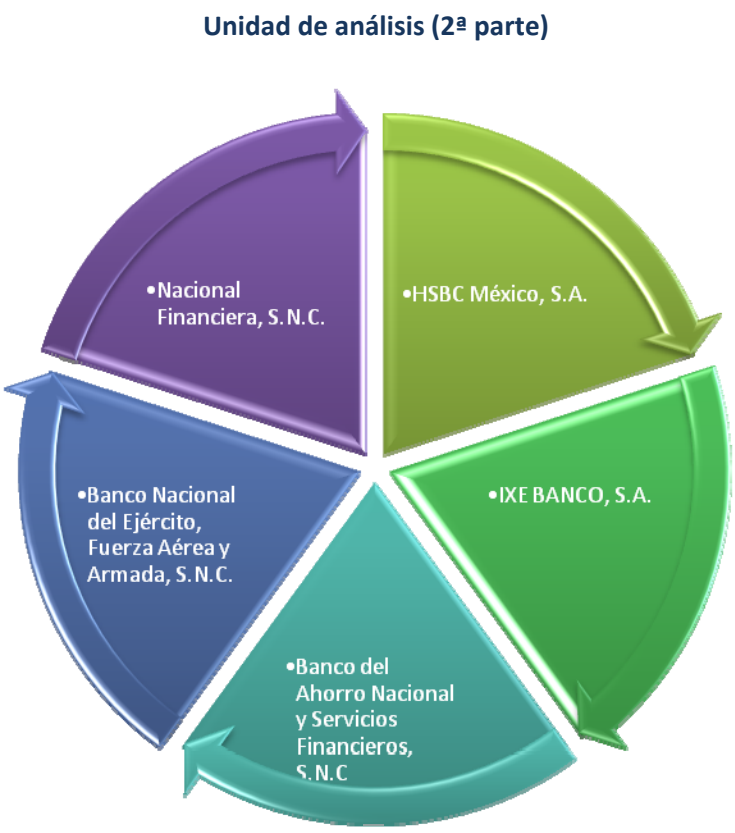


Fig. 29. Unidad de Análisis (2ª parte).

Fuente: Elaboración Propia.

Cabe destacar que el sistema financiero mexicano es coordinado por la Secretaría de Hacienda y Crédito Público, a través de tres Comisiones y del Banco de México, que controlan y regulan las actividades de las instituciones.

A raíz de esta estratificación se tomará en cuenta el ámbito de la actividad productiva de servicios en la cual se tendrá como base el sector financiero debido a que en él no deben existir desmesurables fugas de información y, por ende, se entiende que la difusión acerca de la seguridad de la información en dichas empresas es altamente efectiva; sin embargo, cabe la incertidumbre a dicha suposición y es precisamente dicho punto el que se quiere comprobar.

3.2 LA IMPORTANCIA DE LA SEGURIDAD DE LA INFORMACIÓN EN EL SECTOR FINANCIERO

Para las empresas que forman parte del Sector Financiero en México, el mayor reto de Tecnología de la Información (TI) es proteger la integridad de la delicada información que manejan, mientras cumplen con las regulaciones a las que están obligadas.

La industria financiera mexicana constituida por: bancos comerciales, bancos de desarrollo, grupos financieros, sociedades de inversión, aseguradoras, casas de bolsa, casas de cambio, arrendadoras financieras, afianzadoras, almacenes generales de depósito, uniones de crédito, empresas de factoraje y administradoras de fondos para el retiro (Afores); se enfrenta a una doble tarea que implica retos crecientes para el desarrollo del negocio.

Por una parte, en un sector altamente competitivo todas estas empresas deben garantizar a sus clientes una atmósfera en la que las transacciones financieras en línea se puedan dar de manera segura, protegiendo la delicada información que transmiten, ya que su negocio está basado cien por ciento en la confianza.

Por otro lado, estas empresas deben cumplir una serie de regulaciones siendo que, por sus características, el sector financiero es uno de los sectores más reglamentados, no sólo en México sino también a nivel global y requiere una seguridad de la información adecuada que inhiba la fuga de la misma. Es indudable el vasto potencial de crecimiento que tiene la industria financiera, si se considera que su tamaño es pequeño en relación con el de la economía mexicana.

Según Mexis[19] en un reporte que rindió en mayo del 2009, en el sector específicamente bancario, se ha puesto especial empeño en fomentar la bancarización del país a fin de que, de manera creciente, todos los agentes económicos se conviertan en usuarios de los servicios financieros.

De esta manera existe el enorme reto, por parte de estas instituciones, para ampliar la cobertura del sector alcanzando a más personas y mercados, atendiendo la eficiencia y la seguridad, los dos aspectos medulares que salvaguardan la relación entre las empresas financieras y sus clientes.

Y es que, independientemente de su capacidad económica, todos los usuarios buscan que sus operaciones financieras sean seguras y sin falla. En este punto la plataforma tecnológica juega un papel fundamental.

3.2.1 LA SEGURIDAD: PRIMER REQUERIMIENTO FUNDAMENTAL DE LAS INSTITUCIONES FINANCIERAS

Según el documento “Confianza y garantía: Informe anual de seguridad en instituciones financieras” que la empresa Deloitte publicó en septiembre del 2010, las entidades financieras cuentan cada vez con una

[19] Mexis es una compañía experta en seguridad y redes de datos que mantiene la continuidad operativa de las empresas, puede consultarse en http://www.mexis.net/

gestión más profesionalizada de la seguridad de la información. El aumento de las preocupaciones en materia de seguridad en estas entidades, motivado por aspectos como la sofisticación de los ataques informáticos o la exigencia informativa, han llevado a las entidades financieras a disponer o estar en proceso de implantar una estrategia de seguridad más madura. En dicho informe los principales factores en materia de seguridad en 2010 fueron:

Fig. 30. Principales factores en materia de seguridad en 2010

Fuente: Elaboración propia con base en Informe anual de seguridad en instituciones financieras 2010

de Deloitte.

Como se puede observar encontramos un aumento de la sofisticación de los ataques contra la seguridad, así el malware sigue evolucionando y continúa siendo la principal amenaza externa para las organizaciones. Otro dato reseñable destaca en que se ha incrementado considerablemente la preocupación por la protección de información y prevención de fugas, de hecho, la protección de datos se ha convertido en la segunda prioridad en materia de seguridad para las empresas. Unas empresas que apuestan cada vez más por sistemas integrados de control de acceso e identidades pues las nuevas tecnologías ayudan a rastrear mejor la identidad del usuario y su actividad.

El informe también documenta el aumento de la presión regulatoria en materia de seguridad y gestión de riesgos así como las inversiones en tecnología de seguridad. Además, el trabajo elaborado por Deloitte confirma que el papel sigue estando hasta el final de prioridades para las organizaciones, pues apenas la mitad de las empresas reconocen este formato como un activo de información y muchos de los CISOs siguen sin tener responsabilidad sobre la protección de información en papel y archivos físicos. Asimismo, se hace presente la importancia del CISO así como el incremento en número de empresas bancarias cuyo control presupuestario lo tiene éste.

En cuanto a las tecnologías más implantadas, se mantienen las soluciones de *antivirus, firewalls y antyspam*, destacando la próxima implantación de otras como los sistemas de gestión de vulnerabilidades, el control de accesos a red o la gestión de registros de seguridad.

En formación en seguridad de las empresas, el informe asegura que el 64% de las compañías cuentan con formación específica para identificar y reportar actividades sospechosas que surjan en la organización, pero 1 de cada 5 de estas compañías no hacen nada en este sentido. En lo referido a nuestro país, asegura además que existe una tendencia mayor que en otros países a formar de manera reactiva. Además, se destaca también que los entes con menor formación en materia de seguridad son los ejecutivos y los proveedores externos. Pero hay más datos concretos sobre España, como por ejemplo que las entidades financieras muestran un mayor nivel de implantación de sistemas de medición y *reporting*. A nivel global, sólo 1 de cada 5 compañías dispone de métricas de seguridad y de un sistema de *reporting* regular.

Por otro lado, para el 50% de las empresas, el presupuesto de la seguridad supone menos del 6% del presupuesto de TI. En España ese porcentaje asciende al 67%. Y la difícil situación económica que atraviesa el panorama internacional se hace más patente al comprobar que el porcentaje de empresas que ha reducido el presupuesto de seguridad se ha duplicado respecto a 2009 a nivel global, triplicándose en el caso de España (28%).

Finalmente, en lo que respecta a productos, el software, hardware y consultoría de seguridad son los principales focos de atención de las organizaciones a la hora de distribuir el presupuesto de seguridad. Por el contrario, la formación, la investigación y el desarrollo y gestión de la continuidad del negocio son los rubros que menos recursos económicos reciben.

En un intento de comparación entre el informe retenido en el año 2009 y el obtenido en el año 2010, se puede observar a continuación que, los aspectos que preocupan a las entidades financieras en el 2010 varían ligeramente respecto al estudio pasado, destacando que el gobierno de la seguridad deja de ser una de las prioridades.

Comparación de aspectos importantes para las entidades financieras (2009 vs 2010)

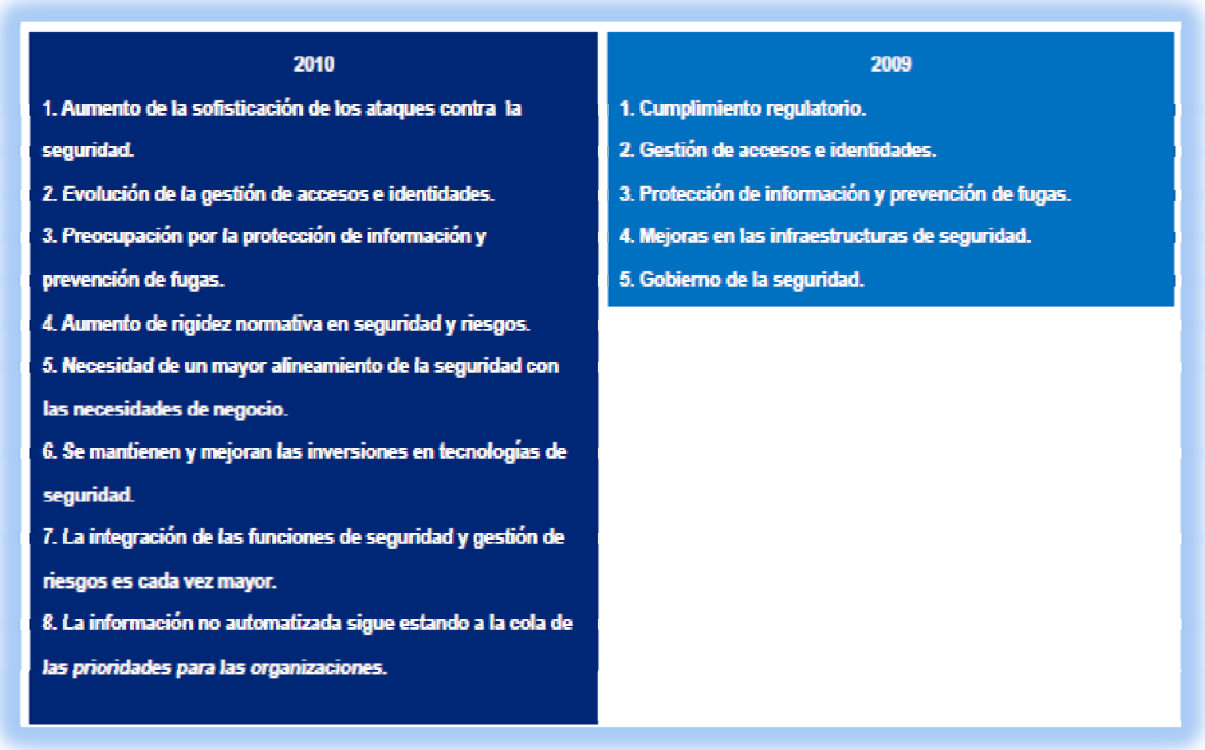


Fig. 31. Comparación de estudios realizados en los años 2009 y 2010.
Fuente: http://profesionaleshoy.es/informe-anual-de-seguridad-en-entidades-financieras/29/09/2010

En resumen, entre las principales conclusiones del informe Deloitte se destaca lo siguiente:

- Existe muestra de una evolución de las preocupaciones en materia de seguridad de la información en las entidades financieras.
- Durante el último año las entidades financieras han percibido un aumento de la sofisticación de los ataques contra la seguridad.
- La figura del CISO crece en importancia. Su nivel de *reporting* es cada vez más ejecutivo y aumenta el número de empresas en las que el CISO tiene el control presupuestario.
- La gran mayoría de las entidades consultadas tiene o tendrá una nueva estrategia de seguridad en los próximos doce meses (año 2011), pero pocas admiten que esté debidamente alineada con los objetivos de negocio.

- Las entidades consultadas confían más en la seguridad de su compañía frente a ataques externos que frente a aquellos que puedan recibir de la propia organización.

- Las tecnologías líderes (más implantadas) continúan siendo las soluciones de antivirus, firewalls o cortafuegos y filtrado de spam (antispam), destacando la próxima implantación de otras como los sistemas de gestión de vulnerabilidades, el control de accesos a red o la gestión de registros de seguridad.

- La gestión de accesos e identidades y la protección de datos se han convertido en las prioridades de las entidades en materia de seguridad de la información.

Éstas son las principales conclusiones del Informe Anual de Seguridad en Entidades Financieras, realizado por Deloitte y en el que han participado más de 350 entidades financieras de todo el mundo, 19 de ellas españolas, la mitad de las entidades participantes en el estudio pertenecen a la región de EMEA (Europa, Oriente Medio y África), un 43% a Norteamérica y Latinoamérica, y el resto a Japón, Asia y Pacífico. El informe, profundiza en la estrategia de las entidades financieras respecto a la organización de la seguridad; la figura del *CISO (Chief Information Secutiry Officer)* y la relación de la función de seguridad con los responsables del negocio, principales preocupaciones en las entidades financieras, evoluciones de presupuestos respecto a la seguridad o principales iniciativas futuras de este tipo de entidades.

Es un hecho que la seguridad es un factor especialmente importante a los ojos de los clientes, cuando los ataques hacia la estructura informática de las organizaciones que forman parte de la industria financiera ya no son producidos por universitarios en busca de notoriedad, sino por delincuentes organizados cuya finalidad es el lucro, los famosos crackers.

Hoy en día, por ejemplo, hay personas que evitan utilizar la banca en línea por temor a que su información sea robada y esto les provoque un daño patrimonial o ponga en riesgo su seguridad personal.

A fin de mantener un ambiente confiable, todos los actores involucrados en la operación segura del sistema financiero mexicano, autoridades, empresas y usuarios, deben hacer su parte. Las autoridades están obligadas a vigilar el cumplimiento de las regulaciones que garanticen un funcionamiento óptimo y actuar en consecuencia si ocurriera lo contrario. Las empresas financieras, por su parte, deben mantener un estricto control interno.

Por último, es necesario que los usuarios se mantengan alertas y sigan al pie de la letra las recomendaciones emitidas por su banco, aseguradora o sociedad de inversión, así como por la Comisión Nacional para la Defensa de los Usuarios de Servicios Financieros (Condusef).

3.2.2 EL ROL QUE JUEGA EL CISO: CHIEF INFORMATION SECURITY OFFICER

En la actualidad las empresas producen un 60% más de información por año y el número de ataques a la misma se incrementa a pasos agigantados, sin embargo, en muchos casos se sigue sin implementar políticas

acorde a este crecimiento. Sin dudas, la información que genera una empresa es uno de los activos más importantes que esta posee. Tener control de las actividades que comprenden uso y generación de información requiere de políticas bien definidas en virtud de garantizar disponibilidad, integridad y confiabilidad de la misma así como contar con una persona que pueda llevar a cabo la planificación de las actividades necesarias para lograr estos objetivos.

De acuerdo con la "Encuesta Global 2007 de Seguridad & Privacidad" de la consultora Deloitte, el 80 % de los ataques que una organización recibe procede de errores humanos.

Al ranking de las brechas de seguridad lo lideran los ataques vía e-mail con un 52%. Luego más abajo se encuentra las actividades víricas con 40%; las actividades de *phishing* con un 35%; la mala conducta de los empleados con un 31%; el *spyware* con 26%, y la ingeniería social con 17%. Es importante destacar que el informe menciona que la efectividad de los ataques internos producidos por los propios empleados es de un 39%.

Asimismo, dicha encuesta, en común acuerdo con el Informe anual de seguridad en instituciones financieras 2010, según sus conclusiones expuestas en el capítulo 3.3.1, menciona que más empresas están optando por tener entre sus filas el rol de CISO cuyas siglas significan *Chief Information Security Officer*. Si sumamos los datos enunciados anteriormente, se puede comprender mucho mejor el por qué de esta decisión, ya que visualizando la seguridad de la información como proceso integral que comprende políticas, procesos orientados al riesgo y enfocados al negocio de la empresa. Se requiere que la coordinación, planificación, organización y control de la información esté en manos de una persona encargada de velar por el cumplimiento de los objetivos de la organización y que éste rol tiene que estar en directa comunicación con el Directorio para poder realizar estas tareas.

El rol que cumple el *CISO* tiene *su actividad principal orientada a garantizar que la información de la organización sea fidedigna y accesible* por los miembros de la empresa que tengan que acceder a ella en base a sus objetivos. Para ello tiene que contar con la posibilidad de implementar las medidas de control que crea conveniente así como coordinar actividades centrado en su misión.

Se pueden detallar las siguientes actividades que estarán bajo el control del *CISO* de acuerdo a un revelamiento llevado a cabo entre las personas que están ocupando dichos cargos en Latinoamerica durante el 1er CISO's Meeting 2005 y que están ordenadas por orden de criticidad.

Lista de actividades bajo el control del Ciso

Fig. 32. Lista de actividades bajo el control del CISO. Fuente: 1er. *CISO´s Meeting 2005*.

Durante mucho tiempo muchas de estas actividades estaban controladas principalmente por el área de sistemas (en el mejor de los casos) contando, en ocasiones, con personal que tuviera conocimientos de seguridad informática.

Las amenazas actuales, así como la cantidad de información que se tiene que gestionar, ha aumentado tan drásticamente que requiere de una verdadera centralización de las decisiones que garanticen lo mejor posible la protección de la información. Estas decisiones principalmente políticas dentro de la organización no tendrían que estar supeditada a la disponibilidad de un área que tiene múltiples actividades asociadas como es el área de sistemas**.**

Es importante entender que *las actividades del* ***CISO no son técnicas totalmente*** y tienen que ser comparadas con las actividades que puede desarrollar un *CEO (CHIEF EXECUTIVE OFFICER)* dentro de la empresa, pero orientada a la información de la misma. Sus conocimientos sí tienen que estar al alcance de comprender cuales son las políticas y procesos necesarios para cumplir con sus tareas.

Como antes se mencionó, su contacto con el Director es algo muy importante a fin de que la comunicación sea directa y que se pueda contar con el apoyo necesario. Este tipo de organización de actores está incluyéndose actualmente como una de las buenas prácticas de seguridad. De esta forma, el Director también podrá estar permanentemente informado de los riesgos que se están incurriendo y así aplicar las medidas adecuadas en caso de ser necesario.

El CISO podrá contar, dependiendo de lo que entienda necesario, con un equipo a cargo de hacer cumplir las políticas y/o tercerizar las partes técnicas a empresas teniendo bajo su cargo el cumplimiento de los objetivos que comprendan las implementaciones que se requieran. Este tipo de relación tiene virtudes muy importantes. Primeramente, *la organización contará con una persona que vele por la seguridad de la información y segundo, reducirá sus costos al tercerizar las actividades de implementación al tiempo que podrá elegir los mejores actores para llevarlas a cabo.*

Por el lado de la empresa que se haya contratado, esta contará con una persona de contacto que tiene poder de decisión dentro de la organización así como la información necesaria para poder realizar el trabajo en el menor tiempo posible y con los mejores resultados dado que no perderá recursos en tratar de dilucidar cuales son los requerimientos.

Como se pudo visualizar en la figura de la lista de actividades del CISO, enunciadas anteriormente, otra de las áreas que están a cargo de éste son las referentes a la seguridad física (control de alarmas de incendio o robo, guardias de seguridad, cámaras, etcétera) dado que no sólo es a través de actividades lógicas que se puede comprometer la seguridad. Para ello podrá contar con herramientas que le permita en todo momento conocer el estado de las distintas dependencias de la organización al tiempo que podrá dirigir las actividades y recursos físicos de seguridad para lograr su objetivo.

A fin de contar con toda la información requerida para cumplir con sus actividades, se puede contar con la implementación de herramientas como los tableros de control, que permitirán tener una visualización general de las actividades y de los incidentes reportados. Para poder mantener esta herramienta, es necesaria una concientización del personal a fin de que los mismos reporten las incidencias de seguridad. Por supuesto, el personal tiene que poder ver el beneficio de este tipo de reportes ya que si no, sólo se sentirán controlados lo que originaría problemas internos al tiempo que podría propender a tratar de saltar los controles instituidos.

Como se puede observar el rol del CISO es de extrema importancia en las decisiones tomadas por la Dirección y que su consulta se hace necesaria para poder cumplir con los objetivos de la empresa al tiempo que se protegen sus activos. Siendo que la Dirección o la alta gerencia no necesariamente tiene que conocer los aspectos fundamentales de la seguridad física y lógica, el contar con un actor como el CISO, permitirá concentrar sus esfuerzos en las actividades que permitan el crecimiento sin comprometer a la seguridad de la organización por el simple desconocimiento.

3.3 MÉTODOS DE SEGURIDAD DE LA INFORMACIÓN IMPLEMENTADOS EN LAS ORGANIZACIONES FINANCIERAS

Los bancos e instituciones financieras son los principales componentes del sistema financiero mexicano. Estos organismos son el último elemento del sistema y son quienes llevan el trato más directo con el público en general. Es por eso que los bancos e instituciones financieras requieren de herramientas tecnológicas altamente eficientes con las cuales puedan llevar a cabo el día a día de las operaciones.

Los clientes de estas instituciones tienden a tener desconfianza al utilizar medios electrónicos para llevar a cabo sus transacciones en línea ya que el flujo principal es el dinero.

Para esto, los bancos e instituciones financieras han ido adoptando una gama de aplicaciones destinadas a satisfacer las necesidades del cliente y a llevar una relación más directa. Términos como CRM e e-Business son cada vez más comunes en este ambiente.

Actualmente, las empresas e instituciones que componen el sistema financiero requieren tener una

avanzada infraestructura tecnológica para poder llevar a cabo todos sus servicios. Estos servicios están compuestos principalmente por tarjetas de crédito, estados de cuenta, cotizaciones en las bolsas de valores, manejos de cuentas, entre otros.

De esta manera las instituciones financieras requieren hacer frente a las demandas de sus clientes de manera satisfactoria, lo que requiere un servicio confiable de tal manera que el cliente deje su dinero en manos de alguna institución. Las tecnologías de información utilizadas por estas instituciones son reguladas por organismos gubernamentales de una manera continua y estricta. En el caso de México estos sistemas son regulados por la Comisión Nacional Bancaria y de Valores.

Debido a esta estricta regulación, estas instituciones deben integrar todos sus sistemas para otorgar a los clientes un servicio de seguridad en el manejo de su dinero. Con herramientas como el CRM[20] las instituciones financieras brindan un mejor servicio a los clientes y aseguran su dinero al tener mayor control sobre el mismo, generando mejores ganancias para la institución y para el cliente.

Para esto existen muchas empresas enfocadas a brindar soluciones para las instituciones financieras.

El objetivo de dicho capítulo es encontrar las características propias de las tecnologías de información utilizadas por las instituciones financieras y la manera que la integración de estas brindan un mejor servicio y seguridad a los clientes.

Para ello se presenta un panorama actual de los componentes que integran el sistema financiero mexicano y se analiza el papel de las TI's en los bancos e instituciones financiera si se propone la implementación de herramientas destinadas a otorgar un mejor servicio al cliente, tales como CRM y e-Business.

3.3.1 EL PAPEL DEL SISTEMA FINANCIERO MEXICANO

El sistema Financiero Mexicano, también conocido como Sistema Bancario Mexicano, se encuentra compuesto por instituciones u organismos interrelacionados que realizan actividades tendientes a la captación, administración, regulación, orientación y canalización de los recursos económicos de origen nacional e internacional como se puede observar en la siguiente figura.

Composición del sistema financiero mexicano

[20] CRM proviene de la sigla del término en inglés "Customer Relationship Management" que traducido al español significa: "La administración basada en la relación con los clientes".

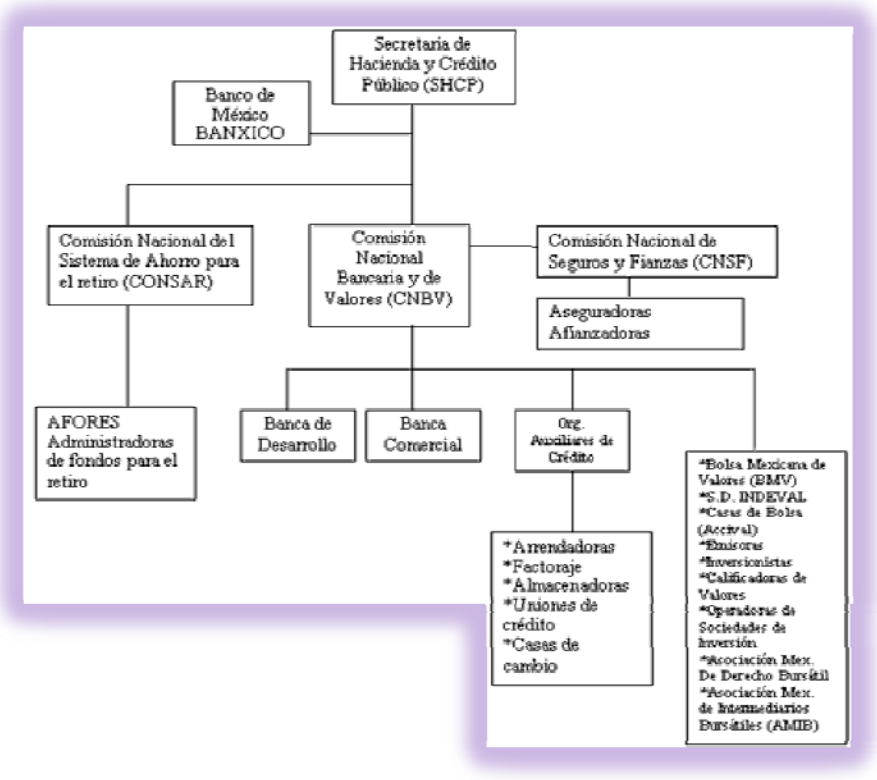


FIg. 33. Composición del Sistema Financiero Mexicano.

Fuente: Diagrama del Sistema Financiero. Recuperado el 1 de noviembre de 2011 en http://www.gestiopolis.com/canales2/finanzas

Estas actividades pueden realizarse por el ahorro o la inversión de las personas físicas y morales, así como por los préstamos solicitados por empresas a través de la emisión de títulos (documentos que valen dinero), mediante los cuales se pretende obtener un beneficio económico a partir de su incursión en alguna de las modalidades del sistema. Por otro lado, los integrantes del sistema reciben beneficios económicos por el desempeño de su actividad.

El Sistema Financiero Mexicano es coordinado por la Secretaría de Hacienda y Crédito Público a través de la CONSAR, la CNBV y la CNSF y del Banco de México, que controlan y regulan las actividades de las instituciones.

Uno de los organismos más importantes es la Comisión Nacional Bancaria y de Valores que coordina y regula la operación de las instituciones de Crédito de la Banca Comercial y de Desarrollo y las Organizaciones Auxiliares de Crédito. Tiene a su cargo la vigilancia y auditoría de las operaciones bancarias y está autorizada para sancionar. La Banca Comercial está integrada por las instituciones encargadas de realizar la intermediación financiera con fines de rentabilidad y constituye el centro de la actividad financiera.

Capta recursos del público con los cuales otorga financiamientos o "créditos" y con esto realiza su función de promover la operación y desarrollo de las empresas como un complemento a la inversión de las sociedades industriales, comerciales y de servicios.

Un banco es la institución de crédito considerada como de banca comercial que tiene como función principal prestar servicios públicos de banca y crédito. Es el punto de contacto entre personas que le confíen dinero y personas que lo solicitan a través de los créditos. La Tabla 3.3.1.1 muestra la evolución de la banca en México.

Evolución de la banca en méxico (1800 – 1900)

Año	Acontecimiento
1821	Consumada la independencia no existe Sistema Financiero
	La Casa de la Moneda y el Monte de Piedad subsisten
1830	Primer Banco: Banco de Avio-Industria Textil.
1837	Banco de Amortización de la Moneda de Cobre.
1854	Se constituye el código de comercio.
1864	Banco de Londres, México y Sudamerica-Capital
1880	Banco de Londres y México-Serfín; y Banco Nacional
1895	Bolsa de México, S. A.
1897	Se promulga la Ley General de Instituciones de Crédito, limita facultades emisión billetes, fija normas para establecer sucursales y otorgar crédito, se reorganiza el S.F.M.
1907	Se reorganiza la Bolsa de Valores de la Ciudad de México; con la revolución, 1910 viene excesiva emisión de papel moneda por cada grupo contendiente. Entra en colapso y deja de funcionar el Sistema Financiero Mexicano.
1914-1916	Diversas Medidas y Decretos por reencauzar el Sistema Financiero Mexicano; emisiones billetes falsos, circulante en metálico.
1917	La nueva constitución establece un nuevo S.F.M. fundado en el monopolio gubernamental de la misión de billetes, bajo la jurisdicción de la SHCP, se organiza el Banco de México, se le dota de facultades-emisión de billetes, fijar tipo de cambio frente a la Comisión Nacional Bancaria y de Seguros. (Ahora separada en CNB y CNSF).
	Banco Central, inician sus operaciones las instituciones nacionales de crédito; Banco Mercantil de Crédito Agrícola , HIP, y de O. Públicas, Banco Mercantil de Comercio Exterior, Nafin., Almacenes Nacionales de Depósito, surgen instituciones privadas.
1925	Banco de México.
1931	Ley Orgánica de Banco de México.
1934	Nacional Financiera.
1946	Reglas y Ordenamientos para que la Comisión Nacional de Valores regule la actividad bursátil.
1975	Ley del Mercado de Valores.
1976	Reglas de Banca Múltiple.
1977	Emisión de Petrobonos.
1978	Emisión de Cetes.
1980	Emisión de papel comercial.
1982	Estatización de la Banca Privada
	Establecimiento del control generalizado de cambios.
1990	Reprivatización, reestablecimiento régimen mixto de servicios de banca y crédito.
1991	Formación de grupos financieros.

Tabla 34. Evolución de la banca en México.
Fuente: Centro Bancario del Estado de Nuevo León.

3.3.2 LOS SERVICIOS FINANCIEROS

El sector de servicios financieros está cambiando rápidamente y está volviéndose altamente competitivo. Las instituciones financieras tratan de proteger su base de clientes, así como de competir por nuevos negocios.

Dichas Instituciones Financieras ofrecen una mezcla de productos y servicios con distintas características entre las que destacan las siguientes:

Características principales de las instituciones financieras

Fig. 35. Características de las Instituciones Financieras.
Fuente: Elaboración propia con base en http://www.gestiopolis.com/canales2/finanzas

Las instituciones financieras cuentan con una variada gama de servicios. Generalmente los servicios financieros son dirigidos a los activos intangibles del cliente, tales como préstamos, productos de inversión.

3.4 EL PAPEL DE LAS TECNOLOGÍAS DE INFORMACIÓN (TI) EN EL SECTOR FINANCIERO

La dinámica del sector financiero se distingue por su marcada competitividad. Para permanecer en este mercado se requiere proveer el mejor servicio y al mejor costo. Este servicio debe ofrecer confiabilidad, disponibilidad, agilidad y calidad de la información. Se requieren tecnologías de información altamente eficientes y capaces de evolucionar de manera flexible y rápida. Así mismo, también se requiere que la inversión en tecnologías sea gradualmente financiable.

El mercado financiero requiere de aplicaciones de alta complejidad y velocidad, ya que su negocio radica en la operación de la información para una adecuada toma de decisiones.

Los analistas bursátiles, los agentes y los profesionales del sector financiero requieren aplicaciones para operar nuevos instrumentos de inversión y crédito.

La tecnología que responde a esta necesidad es la Metodología Orientada a Objetos, misma que logra que la implantación de una aplicación represente el modelo conceptual del diseñador de una manera más natural, esto facilita el diseño de los programas que siendo más extensos, son más comprensibles.

Los costos logran reducirse, ya que la inversión de los sistemas perdura más tiempo y son menores los esfuerzos de programación y mantenimiento (Sin autor, 2004).

3.4.1 LA BANCA ELECTRÓNICA

Internet es un nuevo canal para liberar servicios bancarios. Se requiere una computadora (PC), un módem y un software otorgado por el proveedor de los servicios financieros.

La banca electrónica (e-Banking) significa, según Khalfan Alshawaf (2004), la provisión de información acerca del banco y sus servicios a través de una página en el World Wide Web.

Actualmente los servicios bancarios basados en Internet proveen a los clientes servicios de transacciones tales como accesar a sus cuentas, la habilidad de mover su dinero entre diferentes cuentas, hacer pagos o aplicar para préstamos y otros servicios complementarios.

Debido a la gran competencia existente en el sector bancario, los bancos han tomado gran interés en plataformas electrónicas para la entrega de servicios financieros.

Los mayores beneficios que pretende adoptar y hoy en día está adoptando la banca electrónica se enlistan a continuación:

- Mejor calidad en el servicio al cliente
- Incremento en el número de clientes
- Incremento en las utilidades
- Habilidad para alcanzar un mercado más amplio
- Reducción de costos
- Habilidad para recolectar información del cliente
- Mejorar el uso de los recursos tecnológicos
- Mejorar los procesos de negocio
- Mejores relaciones con los clientes y proveedores
- Mejorar el perfil de la organización
- Entrega rápida de productos y servicios
- Reducción de errores

A pesar de estos beneficios, se ha discutido que la banca electrónica no llena las expectativas de los clientes y fracasa en otorgar lo que el cliente necesita.

La cultura es un factor importante para la banca electrónica. Las naciones son únicas en muchos niveles, desde las preferencias de compra y las preocupaciones por la seguridad hasta la infraestructura de telecomunicaciones nacional y las medidas regulatorias destinadas a proteger el país.

La razón más importante que los usuarios tienen para no hacer uso de la banca electrónica es primordialmente la seguridad, los errores al estar realizando transacciones por medio de Internet, la falta de conocimiento del uso del servicio y renuencia a cambiar la manera actual de hacer trato con los bancos son algunos de los factores que con mayor frecuencia se hacen presentes en la actualidad. Sin embargo, éste paradigma debe evolucionar y las entidades bancarias tienen en sus manos el poder para hacerlo, permitiendo brindar una zona de confort de seguridad al cliente. Por supuesto, el primer paso para realizarlo es el comenzar por ellos mismos, reestructurar su control interno y evitar la fuga constante de información brindando una seguridad mayoritaria en la información, lo que conllevará a la protección de la institución y por consiguiente traerá consigo la plena confiabilidad de los clientes.

3.4.2 CRM, CROSS-SELLING Y SAP

Las tecnologías de información basadas en CRM (Cestones Relationship Managament) y en cross-selling (ventas cruzadas) actualmente tienen una tendencia de crecimiento en los bancos. Gajardo (2004) define al CRM como un modelo de negocios cuya estrategia está destinada a lograr identificar y administrar las relaciones en aquellas cuentas más valiosas para una empresa, trabajando diferentemente en cada una de ellas de forma tal de poder mejorar la efectividad sobre los clientes.

Los bancos han intentado desde instalar sistemas de administración de bases de datos hasta implementar sistemas CRM a través de toda la empresa. La atracción y retención de un cliente valioso es la base de cualquier implementación de CRM.

El *Cross-Selling* es una gran estrategia de mercado para muchas instituciones financieras (Jarrar, 2001).

El objetivo de las ventas a través de sistemas de servicio es entender a los clientes de tal manera que la organización pueda ajustarles cualquier oferta.

Es necesario poner atención en lo que están comprando, en lo que comprarían, en los productos financieros que están comprando en otras compañías, el segmento de mercado en el que se encuentran, la mejor manera de acercarse a ellos, la manera de medir sus reacciones, la manera en asegurar su satisfacción, las habilidades requeridas por el equipo de trabajo, cómo motivarlos, qué sistemas son requeridos para apoyarlos.

En cuanto a la infraestructura tecnológica, existen dos requerimientos principales para asegurar que todas las partes están unidas: los estándares comunes para sistemas centrales, de tal manera que los sistemas separados puedan ligarse, y un banco de datos central accesible para todos.

En este contexto hay dos tipos distintos de tecnologías que apoyan la estrategia de relación con el cliente (Jarrar, 2001):

- CRM: Refiriéndose a sistemas interactivos, tales como apoyo, administración de campañas y automatización de ventas.

- Inteligencia de clientes: La cual provee herramientas para capturar, almacenar, procesar, acceder, organizar y analizar datos de los clientes.

Ésta es el área en donde la mayoría de los bancos no encuentran problemas. Se requiere de una inversión considerable en remendar viejas tecnologías y adquirir nuevos sistemas.

Los sistemas de modelos predictivos construyen modelos de comportamiento para predecir porcentajes de respuestas, oportunidades de cross-selling, potenciales de fraude y candidatos para crédito.

Los bancos deben tener una visión integrada de los clientes, el objetivo de que la información esté integrada es tener un perfil personal y financiero. Los datos que deben estar integrados incluyen: satisfacción de clientes, necesidades del cliente, quejas de los clientes, lealtad de los clientes, perfil personal y financiero del cliente, valores en cartera de los clientes, historial de los contactos hechos con el cliente, segmentación de los clientes y las utilidades generadas por cada cliente.

El peligro potencial es que los bancos veían al CRM como un remedio para el éxito en el futuro. Al implementar un paquete de software para administrar clientes, los negocios pueden mejorar los porcentajes de retención de clientes, incrementar el *cross-selling* y reducir costos. Actualmente, la mayoría de las entidades bancarias cuenta con los famosos SAP´s.

SAP es considerado como el mejor retorno sobre informaciones. Los mercados están cambiando. Los clientes están cambiando. Los negocios están cambiando. El éxito de las compañías depende de la calidad de la información y de la velocidad con que la misma puede ser compartida. Depende de qué tan rápidamente puede responder y adaptarse a los cambios tecnológicos de la compañía.

Se dice que nadie le podrá dar un mayor retorno sobre la información que SAP, quien ha liderado la industria en investigación y desarrollo, gastando en estas actividades un 20% de sus ganancias anuales. Debido a este hecho, SAP ha presentado soluciones innovadoras. Con más de 1000 procesos de negocios incluidos en el software SAP se puede integrar toda la organización; se puede compartir información en tiempo real con los operadores, proveedores y distribuidores, así sea una compañía de 50 o de 100,000 empleados. Por la combinación de un superior conocimiento de negocios y experiencia con las mejores prácticas de la industria, SAP ha brindando grandes soluciones que permiten reestructurar el negocio mientras éste cambia. Hoy en día dicho sistema tiene un gran auge y se espera mucho más de ello en el futuro.

3.4.3 E- BUSSINESS

Durante muchos años las instituciones financieras han desarrollado una serie de herramientas, técnicas y procesos de servicio que tradicionalmente han sido distribuidos por canales.

Los canales remotos han estado en uso por muchos años y la llegada de e-Business ha creado nuevas oportunidades para innovar en términos de productos y canales. En las siguientes secciones se mencionan algunas oportunidades en las cuales la adecuada aplicación de e-Business puede ser de gran utilidad para las instituciones financieras.

Oportunidades relacionadas con los productos financieros

Con los productos financieros puede haber una gran variedad de oportunidades, entre las que destacan:

Productos dinámicos: Los productos financieros pueden ser manejados de una manera más fluida. Por ejemplo, los clientes pueden cambiar los atributos de sus tarjetas de crédito vía Internet, pueden mover su dinero desde un producto financiero a otro, compensar un saldo deudor con uno acreedor.

Sitio Web personalizado y agregación: Las cuentas de agregación son definidas como una recolección de información proveniente de diferentes fuentes en línea para desplegarla en una sola pantalla.

Utilizando este tipo de cuenta, los clientes pueden ver detalles de varias de sus cuentas en línea y otra información en línea que sea de utilidad. La información presentada al cliente puede ser sobre sus cuentas bancarias, cuentas de ahorro, detalles de créditos, su portafolio de inversiones, servicios personalizados y correo electrónico.

Diferenciación de productos: Los productos financieros como las cuentas, y las tarjetas de crédito y débito, tienen poca diferencia en cuanto a costos. Las instituciones financieras tratan de que estos productos tengan una diferenciación en cuanto al valor agregado de sus servicios.

Esto es posible a través de las cuentas basadas en transacciones en línea en donde puede haber una oportunidad para los proveedores del servicio para otorgar al cliente mensajes y para personalizar el uso de su interfaz (Boyes, Stone, 2003).

Portabilidad del producto: Se busca la portabilidad del producto, las soluciones aplicadas a las cuentas actuales pueden ser transferidas a otros productos financieros que tradicionalmente son incómodos de cambiar. Con el *e-business* los productos financieros se entregan de una manera más agilizada, otorgando al cliente comodidad y agilidad en sus transacciones.

Oportunidades relacionadas con los canales

En cuanto a las oportunidades con los canales de comunicación, es posible encontrar las siguientes oportunidades:

Funcionalidad ATM (Modo de transferencia asincrónica): La funcionalidad ATM puede ser desarrollada para permitir a los clientes completar aplicaciones para préstamos, tarjetas de crédito, hipotecas, etc. (Boyes, Stone, 2003).

Voz sobre el protocolo de Internet: Las tecnologías basadas en Internet han traído rápidamente servicios de voz basados en la Web, que ha sido utilizado por las compañías para llevar a cabo reuniones corporativas, conferencias y seminarios. Esta tecnología puede ser utilizada en la distribución de productos financieros.

Rama del futuro: La conveniencia y el confort se están volviendo más importante al mismo tiempo en que las instituciones financieras tratan incrementar su participación en la cartera del cliente.

Presentación de la factura electrónica y el pago: A través de este sistema, las transacciones de dinero pueden ser sostenidas electrónicamente a través de Internet, desde emitir la factura hasta recolectar el pago.

Comunicaciones móviles: Las instituciones financieras buscan migrar las transacciones, productos y servicios al cliente a canales más baratos. Con canales de comunicación más eficientes, es posible realizar un gran número de operaciones y transacciones en el menor tiempo.

Oportunidades relacionadas con el riesgo

Las oportunidades relacionadas con el riesgo del negocio se refiere a la seguridad con que la que se realizan las transacciones. Dichas oportunidades son las siguientes:

Seguridad del cliente: Las instituciones financieras pueden tomar los pasos para elevar el perfil de seguridad y educar a los clientes en temas de seguridad.

Firmas digitales: Las instituciones financieras pueden moldear los estándares de las firmas digitales.

Actualmente, se le da gran importancia a la seguridad al momento de realizar transacciones, ya que frecuentemente se presentan casos de fraude por la falta de seguridad en las transacciones en línea.

Oportunidades relacionadas con la mercadotecnia

Uno de los tópicos más importantes en todo E-Business es el relacionado con el de la mercadotecnia, dentro de las oportunidades se encuentran:

Mercadotecnia del sitio: Estos sitios pueden ser utilizados para desarrollar nuevas remuneraciones y beneficios para el personal.

Mercadotecnia y marcas en Internet: Internet, el teléfono celular y la televisión interactiva pueden crear nuevos caminos para entregar marcas que no sean copias de aproximaciones tratadas y probadas en aplicaciones convencionales.

Una buena imagen de cualquier sitio llama la atención y crea confianza en los usuarios: Es de suma importancia contar con el asesoramiento requerido para que los sitios reflejen una buena imagen de los servicios.

Quisiera finalizar el presente capítulo exponiendo que el ambiente que se vive dentro del sector financiero es de alta competencia; es por eso que las instituciones financieras deben buscar los mecanismos adecuados para acercarse a los clientes y generarles la confianza requerida para que ellos elijan los servicios.

Ésta es la razón por la cual día con día estas instituciones implementan sus tecnologías de información con las herramientas más adecuadas para conservar la lealtad de los clientes. Actualmente los clientes buscan seguridad al momento de realizar sus transacciones de manera electrónica y lo hacen demandando canales de comunicación más eficientes con el flujo ágil de la información; las instituciones financieras han ido adoptando una nueva manera de trabajar y de asegurar los activos de sus clientes.

Con estas herramientas cada vez más clientes utilizarán estos medios electrónicos en sus operaciones y conservarán el servicio que más se adapte a sus necesidades en el corto plazo.

3.5 LA RELACIÓN DE LA INGENIERÍA SOCIAL CON EL SECTOR FINANCIERO

Hasta el momento se ha hablado de seguridad física y lógica, pero, ¿qué hay de los activos intangibles? ¿Acaso las personas que laboran en las instituciones bancarias no son importantes?

Aunque parezca redundante, es importante destacar que las entidades bancarias dentro del sector financiero han invertido cuantiosas sumas de dinero en la implementación de herramientas físicas y lógicas que inhiben el paso de entes no autorizados y claro, cumplen su función; sin embargo surge la cuestión del porqué aún se presentan continuos fraudes y fugas de información.

¿Qué hay de aquellas personas que laboran en las instituciones bancarias?, aquéllas que no se sienten identificados y partícipes de la organización, lo que coloquialmente conocemos como "ponerse la camiseta", o si lo hacen, frecuentemente son partícipes de fraudes de manera involuntaria debido al escaso conocimiento que se tiene referente al tema de la ingeniería social y de la cultura de seguridad de la información que la conlleva.

Es por ello, que dicho capítulo expondrá esté vínculo tan estrecho que existe entre la ingeniería social y el sector financiero, ya que tanto empleados como clientes han sido víctimas sustanciales del robo de información por parte de crackers que buscan un beneficio económico mal habido el cual es recompensado por los individuos que desean la información confidencial y relevante de la mayoría de las entidades bancarias. Una forma de ataque que bien puede afectar tanto a clientes como a empleados de las mismas entidades bancarias.

Como bien se ha mencionado en el Capítulo 2, el método de la ingeniería social varía dependiendo del entorno, pero siguen un patrón constante, el cual se divide de manera generalizada en tres puntos fundamentales que se enuncian a continuación:

- **Fase de acercamiento para ganarse la confianza del usuario:** Esto se hace haciéndose pasar por un integrante de la administración, de la compañía, del círculo social, o por un cliente, proveedor, etcétera.

- **Fase de alerta, para desestabilizar al usuario y observar la velocidad de su respuesta.** Por ejemplo, éste podría ser un pretexto de seguridad o una situación de emergencia en la que se busca que la víctima revele información de gran importancia al creer que hace un bien para inhibir la emergencia que el atacante planteó.

- **Una distracción,** es decir, una frase o una situación que tranquiliza al usuario y evita que se concentre en el alerta. Ésta podría ser un agradecimiento que indique que todo ha vuelto a la normalidad, una frase hecha o, en caso de que sea mediante correo electrónico o de una página Web, la redirección a la página Web de la compañía. Con esto el atacante podría ganar tiempo ya que tranquilizó al a víctima para que no tome las medidas pertinentes al encontrarse ante un posible riesgo o amenaza.

Cabe destacar que la ingeniería social puede llevarse a cabo a través de una serie de medios tales como: teléfono, correo electrónico, correo tradicional, mensajería instantánea, etcétera.

La seguridad informática busca garantizar que los recursos de un sistema de información sean utilizados tal como una Organización o un usuario lo ha decidido. La información es el elemento principal a proteger, resguardar y recuperar dentro de las redes empresariales.

Una de las preocupaciones de la seguridad de la información es proteger los elementos que forman parte de la comunicación, por lo cual es necesario identificar los elementos que la seguridad de la información busca proteger:

Elementos que la seguridad de la información busca proteger

Fig. 36. Elementos que la seguridad de la Información busca proteger.
Fuente: Elaboración propia.

¿Quién representa el punto débil en seguridad?

Ésta es una de las cuestiones que más atañe a nuestras inquietudes, el saber quién es la entidad más vulnerable que permite esa fuga de información y la respuesta se muestra en la siguiente imagen.

Representantes del punto débil en la seguridad

Fig. 37. Representantes del punto débil en la seguridad.
Fuente: Elaboración propia.

Son precisamente los que representan la última línea de defensa los que deben iniciar la seguridad en cualquier lugar y a los cuales se les debe instruir con una cultura de seguridad de la información para se encuentren a la expectativa y sepan detener esas fugas de información prominentes.

La seguridad no se trata sólo del trabajo de personas dedicadas a ello; también requiere la interacción de los usuarios. Son ellos, más que los expertos, quienes pueden prevenir que un sistema sea atacado, vulnerado o comprometido.

Es importante que los usuarios tengan conciencia de las medidas de seguridad básicas, pues así protegen sus datos y los de la organización.

3.5.1 ATAQUES FRECUENTES EN EL SECTOR FINANCIERO FUNDAMENTADOS EN LA INGENIERÍA SOCIAL: MALWARE

La palabra Malware proviene del término en inglés *Malicious Software*, y en español es conocido con el nombre de código malicioso. Malware es un término general con el que se hace referencia a todo aquel software que perjudica a la computadora, dicho ataque tienes distintas vertientes, las cuales se enuncian a continuación:

Virus

El virus es un código malicioso que se propaga o infecta insertando una copia de sí mismo en otro programa para convertirse en parte de él. Un virus no puede ejecutarse por sí mismo, requiere que el programa que lo aloja sea ejecutado para poder realizar sus operaciones.

Este tipo de ataque puede dañar o eliminar datos del equipo, usar el programa de correo electrónico para propagarse a otros equipos o incluso borrar todo el contenido del disco duro.

Caballos de Troya (Troyanos)

Los Caballos de Troya, o comúnmente conocidos como Troyanos, son programas que aparentan ser una aplicación confiable, pero en realidad contienen una acción maliciosa en contra del usuario.

Estos programas podrían dañar nuestro equipo cuando descargamos un programa para cierta función que deseamos que realice, o bien de sitios Web no confiables, esto es, no oficiales o que no cuentan con algún mecanismo de autenticidad como el intercambio de certificados. Esto implica que estamos propensos a descargar un programa troyano. Otra manera de poder adquirir uno de estos códigos maliciosos es mediante correo electrónico, cuando recibimos mensajes de remitentes desconocidos que nos piden que descarguemos un archivo adjunto. Además de esto día a día las técnicas que usan los intrusos evolucionan y actualmente los troyanos son muy sofisticados y pueden funcionar como *"backdoors o puertas traseras"* para abrir un canal de comunicación que permite al intruso conectarse a nuestro equipo y manipularlo remotamente sin que nosotros estemos conscientes de ello. Finalmente, cabe destacar que, para protegerse de un troyano, es necesario contar con un software antivirus actualizado, contar con un software antispyware, aplicar las actualizaciones de seguridad a nuestro equipo constantemente, no descargar archivos adjuntos de correos desconocidos ni descargar archivos de sitios Web no confiables.

Gusanos de Internet (Worms)

Los "Gusanos", o mejor conocidos como "*Worms*", son un código malicioso autopropagable, el cual puede distribuirse a sí mismo a través de una conexión de red, se propaga de computadora a computadora y tiene la capacidad a extenderse sin que el usuario lo ejecute. Puede tomar acciones dañinas tales como consumir recursos de sistemas de red o locales, causando posiblemente un ataque de negación de servicio (*DoS*).

Spyware

El Spyware es también conocido como "programa espía" y comúnmente se refiere a aplicaciones que recopilan información sobre una persona u organización.

El objetivo principal del spyware es recolectar información sobre el usuario y distribuirlo a empresas publicitarias u otras organizaciones interesadas.

Cuando este tipo de software es instalado en un equipo podría enviar ventanas de mensajes emergentes, redirigir el navegador Web a ciertos sitios, o monitorear los sitios Web que son visitados. En casos extremos, algunas versiones de spyware podrían registrar lo que el usuario escribe desde el teclado a través de otros programas maliciosos como los famosos keyloggers.

Debido al procesamiento extra que genera el spyware, el equipo de cómputo podría disminuir su rendimiento, volviéndose extremadamente lento.

Bots

Un *bot*, o robot informático, permite a un atacante obtener el control completo sobre un equipo. Los equipos que están infectados con un "bot" son generalmente denominados equipos zombie. Una "botnet" es una red de equipos zombie que un atacante utiliza para distintos fines maliciosos

Una de las mejores defensas contra amenazas como éstas es ejecutar anti-virus y anti-spyware en las computadoras. También debe asegurarse de mantener su sistema operativo y las aplicaciones parchadas contra vulnerabilidades conocidas y utilizar un programa de firewall personal de algún tipo para proteger al equipo de accesos no autorizados.

Phishing

Este es uno de los ataques que con mayor frecuencia se encuentra a la expectativa del sector financiero, ya que compromete la confidencialidad de los tanto del personal que laboran en las entidades bancarias como de los clientes que hacen uso de las mismas. Dicho ataque tiene el propósito de robar información personal de un usuario y poder suplantar su Identidad.

El *phishing scam o phishing* consiste en la capacidad por parte de un intruso de duplicar una página Web para hacer creer al usuario que se encuentra accediendo a la página Web original de su correo electrónico, institución financiera, tienda departamental, institución académica, etc., y no a una página Web falsa alojada en un servidor controlado por él.

Esquema de ataque de tipo phishing

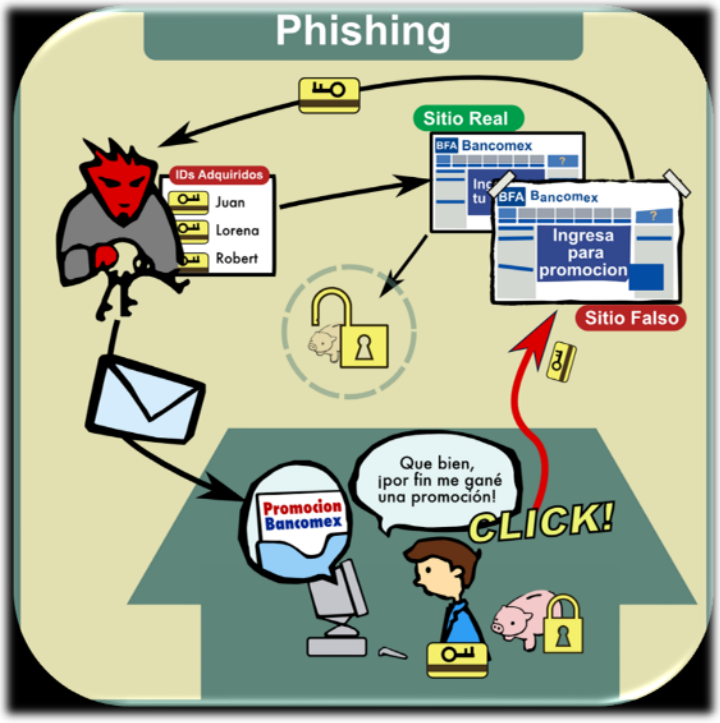


Fig. 38 Esquema de ataque de tipo Phishing.
Fuente: Congreso de Seguridad 2010.

Pharming

Al igual que el Phishing, el Pharming es uno de los ataques cuya frecuencia en el sector financiero ha tenido gran auge en los últimos años. Su intención es que un usuario abra un archivo malicioso en su computadora para que este ocasione un cambio en el equipo capaz de dirigir al usuario a un sitio falso.

Es el acto de explotar una vulnerabilidad en el software de un servidor de DNS,[21] que permite que una persona se adueñe del dominio de un sitio Web, por ejemplo, y redirija el tráfico hacia otro sitio.

Este tipo de ataques normalmente comienzan con el envío de un correo electrónico que aparenta ser de una institución de confianza, por ejemplo un banco, periódico, institución educativa, gobierno, servicios de tarjetas postales, etcétera.

[21] Domain Name System o DNS (en español: sistema de nombres de dominio) es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada.

Esquema de ataque de tipo pharming

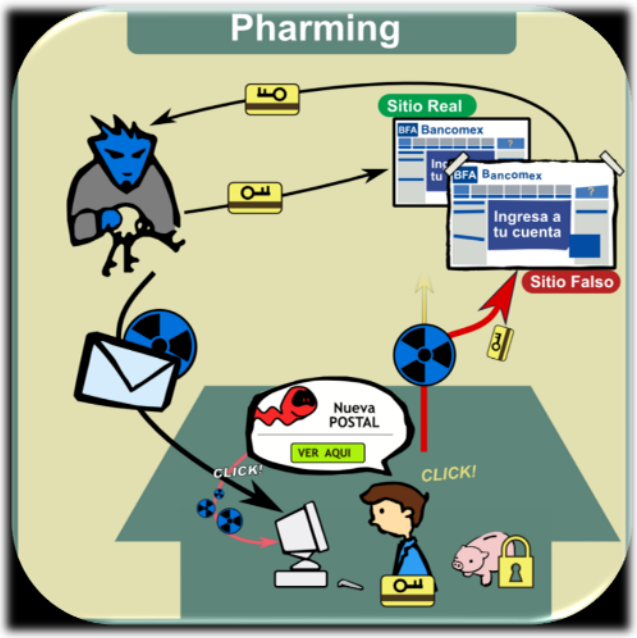


Fig. 39. Esquema de ataque de tipo Pharming.
Fuente: Congreso de Seguridad 2010.

Spam

El Spam es la versión electrónica del "correo basura". Este término se refiere a mensajes de correo electrónico no solicitado, a menudo llamado también correo electrónico no deseado.

Por lo regular este tipo de correos son enviados de manera masiva. No necesariamente contiene virus, ya que algunos son mensajes válidos desde fuentes legítimas que podrían caer dentro de esta categoría; regularmente su contenido está relacionado con el anuncio o venta de un producto.

Aunque el spam puede distribuirse a través de distintos medios, el más utilizado por parte de los spammers está basado en el correo electrónico. Otras tecnologías de Internet que han sido objeto de spam incluyen mensajes de texto, grupos de noticias, usenet, motores de búsqueda, blogs, mensajería instantánea y también los teléfonos celulares.

En resumen, la Ingeniería Social busca obtener datos confidenciales a través de la manipulación de usuarios. Esto lo pueden hacer investigadores privados, criminales, o delincuentes computacionales, para obtener información, acceso o privilegios en sistemas de información de las organizaciones y principalmente de aquellas que tienen un compendio interesante del cual puedan substraer beneficio.

Debemos ser muy precavidos y principalmente las instituciones financieras, ya que como se mencionó con anterioridad, el eslabón más débil es el ser humano. Concientizar a los empleados y clientes de dichas entidades para que hagan un buen uso de la información y puedan protegerla o por lo menos amenorar el índice de ataques que hoy en día se encuentran presentes a nuestro alrededor, no es tarea fácil, pero poniendo de nuestra parte y con un cambio de paradigma en la cultura de seguridad de la información lo lograremos.

3.6 USO DE DISPOSITIVOS MÓVILES EN EL SECTOR FINANCIERO

Actualmente contamos con un repertorio variado de distintos dispositivos móviles como PDA, IPAD, Treo, smartphones, teléfonos celulares y terminales como punto de venta inalámbricas; en las que se puede conectar un sinfín de aplicaciones móviles para beneficios de empresas e individuos.

El celular es uno de los objetos personales más apreciados, de acuerdo con un estudio realizado en el 2007 por la Asociación Mexicana de Internet (Amipci) titulado "Usuarios de Internet en México y Uso de Nuevas Tecnologías 2007". Los usuarios cibernautas consideran al móvil como el segundo medio indispensable (81%), sólo por debajo de Internet (92%). La Televisión TV se encuentra en tercer lugar, con 60%, y las revistas van en último sitio, con un 19%.

Una de las razones por las que la tecnología celular ocupa esta posición de preferencia entre los usuarios, radica en su capacidad de comunicación mediante el uso de mensajes SMS. El 36% de los encuestados por dicha asociación envía entre uno y 25 mensajes al mes, y 31% manda más de 50.

Hoy en día, más del 40% de los ejecutivos están al menos un 20% de su tiempo fuera de la oficina. Según datos de IDC, el número de trabajadores móviles alcanza ya un 40% a escala global. Se tuvo una estimación para el año 2011, de acuerdo con Gartner, de que el 50% de los celulares fueran teléfonos inteligentes y hoy en día lo podemos comprobar, ya que el mercado rebasa dicho porcentaje.

Asimismo, de acuerdo con resultados de la tercera Encuesta Anual de Consumidores de Autoservicio de NCR, realizada en Estados Unidos y Canadá por *BuzzBack Market Research*, "86% de los consumidores dicen que es más probable tener tratos comerciales con empresas que ofrecen la flexibilidad de interactuar utilizando el autoservicio, sea a través de Internet, con un aparato móvil o a través del cajero automático".

Tal encuesta muestra claramente que los consumidores aprecian la posibilidad de usar una combinación de canales como PDA, smartphone, ciberespacio, cajeros ATM y/o kioskos, con el propósito de mejorar su experiencia.

Si se pueden enviar correos electrónicos, navegar por internet y hasta disfrutar de TV en línea con los dispositivos móviles actuales, ¿por qué no revisar el estatus de una orden de compra, rellenar reportes de gastos, revisar los resultados de las ventas o actualizar el sistema de rotación de inventarios?

Más importante aún, muy pronto, la telefonía celular y otros dispositivos móviles se transformarán en innovadores medios de pago. El núcleo de esta transformación radica en un floreciente ecosistema de

aplicaciones empresariales en desarrollo, que permiten un entorno móvil, flexible y práctico para realizar transacciones comerciales.

Según una investigación realizada por *Juniper Research*, se estimaba que cerca de 52 millones de consumidores adoptaran modelos de pago móvil para 2011. Tan sólo en el vecino país del norte, el mercado hispano es muy propenso a adoptar este tipo de servicios para operaciones de envío de remesas.

La posibilidad de ofrecer micropagos mediante aplicaciones móviles generará nuevas formas de interacción entre organizaciones e individuos. Pequeños pero constantes egresos a nivel masivo, permitirán servicios que incluyen comprar alimentos, pagar por descargas de música o adquirir el periódico. Lo mejor es que todas estas transacciones podrán ser utilizadas por personas no bancarizadas, lo que extenderá significativamente la penetración del servicio financiero entre la población de escasos recursos.

El mercado es prometedor. De acuerdo con el CGAP, un consorcio de organizaciones dedicado a expandir el acceso a servicios financieros entre la gente menos favorecida, 59% de los más de 2,000 usuarios móviles viven en países en vías de desarrollo; muchos todavía no están dentro del sistema bancario formal.

Sin embargo, el motor de los cambios a operar no está en la filantropía. La posibilidad de ofrecer transacciones por vía celular podría costar hasta seis veces menos que una operación por ventanilla. Esta es, sin duda, una ventaja que la industria no va a dejar pasar por alto.

Dice Juan Carlos Vera, director regional de *Sysgold Wireless México*, que actualmente hay dos tipos de mercado para las aplicaciones de movilidad empresarial: el horizontal, representado por soluciones de push e-mail, y el vertical, liderado por el sector de consumo desde su origen (con las industrias refresquera y cervecera como las pioneras).

Pero ahora está entrando una segunda ola de crecimiento, “con el sector farmacéutico como el protagonista, seguido por la utilización de dispositivos móviles (como PDA y smartphones) en los nichos financiero y gubernamental”, comenta el ejecutivo, quien considera que en un par de años los censos del Inegi podrían recurrir a este tipo de soluciones para agilizar el levantamiento de datos, “tal como ya se hace en otros países, con importantes ahorros en procesamiento y captura de la información”.

En el ínter de la transición, dos sistemas prevalecen hoy en día. El primero es el llamado “pago por proximidad”, que incluye abonos a corta distancia mediante tecnologías como rayos infrarrojos, bluetooth, chip sin contacto, tarjetas inteligentes, de interfaz dual y/o Wi-Fi. El segundo sistema es el de pagos remotos, caracterizado por desembolsos más convencionales a través de una red abierta como Internet.

En este contexto de competencia, distintas opciones intentan imponerse. Tal es el caso de tecnologías como bluetooth e identificación por radiofrecuencia (RFID), así como otras más nuevas: la especificación zigBee, que define soluciones para las comunicaciones inalámbricas a bajo costo; UWB (Ultra Wide Band), y NFC *(Near Field Communications).*

Incluso, es posible combinar arquitecturas y plataformas diversas, con el propósito de hacer un uso óptimo de todo tipo de aparatos (Blackberry, PDA, teléfonos con sistemas operativos diversos, etcétera), que en ocasiones constituyen ecosistemas poco homogéneos al interior de las organizaciones.

3.6.1 EL MOVIMIENTO DE LOS BANCOS

"A corto plazo, abunda Vera, muy seguramente veremos un mayor uso de dispositivos móviles por parte del sector bancario, que se muestra muy interesado en desarrollar soluciones alternativas que permitan emplear aparatos como los teléfonos móviles, con el propósito de realizar ciertas transacciones y consultas".

"El portafolio de soluciones IT disponibles hace posible el desarrollo de ciertas actividades financieras sin necesidad de que el cliente visite físicamente su entidad bancaria. Ahora serán los bancos quienes se acerquen a sus clientes y prospectos", ahonda. "Nuestros estudios muestran que podemos ayudar a los bancos a incrementar 25% su colocación de productos financieros, reducir sus costos operativos hasta 20% y disminuir las tasas de rechazo de solicitudes crediticias en, al menos, 35%, entre otros tantos beneficios".

Cooperativas de crédito y ahorro, como Coopeuch (en Chile), y bancos como Citibank y ABN AMRO (en Brasil), son algunos ejemplos de entidades financieras a la vanguardia de servicios mediante dispositivos móviles. Estas instituciones han mejorado sus procesos y reducido su ciclo comercial de semanas a días, e incluso horas.

A pesar de que aún hay obstáculos por sortear (la seguridad de las transacciones, sin duda, uno de los principales) la búsqueda de estándares se está intensificando, las alianzas empresariales se van fortaleciendo y las aplicaciones empresariales de movilidad siguen prosperando.

Pero, ¿qué sucede con el uso de dispositivos dentro de las entidades bancarias por parte de los empleados? ¿Acaso inhibir el uso de dicho dispositivo en jornadas de trabajo dentro del sector financiero sería bueno? ¿Qué pasaría con las constantes fugas de información que se presentan a diario?, ya que, si bien es cierto que dichos dispositivos facilitan las acciones cotidianas, también podría ser un medio muy palpable, fácil y rápido para difundir información confidencial, ya sea de manera intensional o inconsciente, pudiendo facilitar información que podría ser empleada con fines maliciosos.

A ello se une el famoso dicho, "Predicar con el ejemplo", ya que sería incongruente que las entidades bancarias difundan a sus clientes el uso de tecnologías a través de dispositivos móviles y lo inhiban para los miembros de su corporativo ¿No lo creen? Será interesante ver esos resultados.

IV. METODOLOGÍA

4.1 TIPO DE ESTUDIO

La tipología que se empleó para la elaboración del protocolo de investigación fue mixta, ya que se tomaron en consideración los siguientes tipos de investigación:

Es un estudio *descriptivo* debido a que nos interesó conocer las características más importantes de la población de las instituciones financieras mexicanas de Banca Múltiple y de Banca de Desarrollo en el Distrito Federal.

De tipo *transversal* ya que se tomó la muestra de la población de las instituciones financieras mexicanas de Banca Múltiple y de Banca de Desarrollo en el Distrito Federal, con base en las variables propuestas para conocer la susceptibilidad de dicha población ante la técnica de la Ingeniería Social en un momento dado, para fines de esta investigación el periodo fue de noviembre de 2011 a febrero de 2012.

Finalmente, el estudio se consideró *predictivo*, ya que de cierta manera se realizó una estimación del nivel de seguridad de la información y del conocimiento con los que cuentan las entidades financieras mexicanas en el presente y que de no tomar cartas en el asunto, en un futuro, los hackers/crackers, aplicando la técnica de la Ingeniería Social, serán un blanco fácil de ataques informáticos que atenten contra la seguridad de la información.

4.2 DISEÑO DE INVESTIGACIÓN

4.2.1 ETAPAS

Las etapas del diseño de investigación se muestran en el diagrama siguiente:

Fig. 40. Esquema de Investigación.

Fuente: Elaboración propia.

4.3 POBLACIÓN O UNIVERSO

La población a considerar para dicha investigación fueron las Instituciones financieras de Banca Múltiple y de Banca de Desarrollo mexicanas pertenecientes al área del Distrito Federal. Para ello se tomaron en consideración los datos del padrón de identidades financieras supervisadas por la Comisión Nacional Bancaria y de Valores CNBV,[22] los cuales se enuncian a continuación:

INSTITUCIONES DE BANCA MÚLTIPLE	INSTITUCIONES DE BANCA DE DESARROLLO
AMERICAN EXPRESS BANK (MEXICO), S.A.	BANCO DEL AHORRO NACIONAL Y SERVICIOS FINANCIEROS, S.N.C.
BANCA AFIRME, S. A.	
BANCA MIFEL, S.A.	BANCO NACIONAL DE COMERCIO EXTERIOR, S.N.C.
BANCO ACTINVER, S.A.	
BANCO AHORRO FAMSA, S.A.	BANCO NACIONAL DE OBRAS Y SERVICIOS PUBLICOS, S.N.C.
BANCO AMIGO, S.A.	
BANCO AUTOFIN MEXICO, S.A.	BANCO NACIONAL DEL EJÉRCITO, FUERZA AEREA Y ARMADA, S.N.C.
BANCO AZTECA, S.A.	
BANCO COMPARTAMOS, S.A.	NACIONAL FINANCIERA, S.N.C.
BANCO CREDIT SUISSE (MEXICO), S.A.	
BANCO DEL BAJIO, S.A.	SOCIEDAD HIPOTECARIA FEDERAL, S.N.C.
BANCO FACIL, S.A.	
BANCO INBURSA, S.A.	
BANCO INTERACCIONES, S.A.	
BANCO INVEX, S.A.	
BANCO J.P. MORGAN, S.A.	

[22] CNBV: Comisión Nacional Bancaria y de Valores (2012). Instituciones que conforman la Banca Múltiple y la Banca de Desarrollo en México. Consultada el 15 de julio del 2011 en http://www.cnbv.gob.mx/Paginas/Index.aspx

BANCO MERCANTIL DEL NORTE, S.A.	
BANCO MONEX, S.A.	
BANCO MULTIVA, S.A.	
BANCO NACIONAL DE MEXICO, S.A.	
BANCO REGIONAL DE MONTERREY, S.A.	
BANCO SANTANDER (MEXICO), S.A.	
BANCO VE POR MAS, S.A.	
BANCO WAL-MART DE MEXICO ADELANTE, S.A.	
BANCOPPEL, S.A.	
BANK OF AMERICA MEXICO, S.A.	
BANK OF TOKYO-MITSUBISHI UFJ (MEXICO), S.A.	
BANSI, S.A.	
BARCLAYS BANK MEXICO, S.A.	
BBVA BANCOMER, S.A.	
CIBANCO, S. A.	
DEUTSCHE BANK MEXICO, S.A.	
HSBC MEXICO, S.A.	
ING BANK (MEXICO), S. A.	
INTER BANCO, S.A.	
IXE BANCO, S.A.	
SCOTIABANK INVERLAT, S.A.	
THE BANK OF NEW YORK MELLON, S.A.	
THE ROYAL BANK OF SCOTLAND MEXICO, S.A.	
UBS BANK MEXICO, S.A.	
VOLKSWAGEN BANK, S.A.	

Fig. 41. Padrón de Entidades de Banca Múltiple y de Banca de Desarrollo Supervisadas por la Comisión Nacional Bancaria y de Valores.

Fuente: Elaboración propia con base en la Comisión Nacional Bancaria y de Valores – CNBV.

4.3.1 UNIDAD DE ANÁLISIS

La unidad de análisis se centró en las siguientes propuestas de Instituciones Bancarias ubicadas en el Distrito Federal y cuyo sector se aboca a las Instituciones financieras de Banca De Desarrollo e Instituciones Financieras de Banca Múltiple, dichas empresas se enuncian a continuación:

4.3.1.1 BANCO SANTANDER (MÉXICO), S.A.

Banco Santander es una institución de Banca Múltiple que cuenta con un modelo de negocio centrado en el cliente que le permite mostrar una gran recurrencia en sus ingresos y resultados, a pesar de las dificultades del entorno económico y financiero de los últimos años. Este modelo de negocio se centra en cinco pilares: Orientación Comercial, Eficiencia, Diversificación geográfica, Prudencia en riesgo y Disciplina de capital y fortaleza financiera.

Además, Banco Santander mantiene un firme compromiso con la sociedad en todos los países en los que está presente. Su principal apuesta es Santander Universidades que cuenta con 833 convenios de colaboración con universidades de todo el mundo. Otras acciones de RSC en medio ambiente y acción social demuestran el firme compromiso del Banco con el desarrollo sostenible. Todo esto, posiciona a la marca Santander como una de las más valoradas del sector financiero (tercera del mundo según la publicación Brand Finance). La marca Santander representa los valores que convierten al Grupo en único: dinamismo, fortaleza, innovación, liderazgo, orientación comercial y ética profesional.

Se encuentra ubicada en Prol. Paseo de la Reforma núm. 500. Col. Lomas de Santa Fe. Distrito Federal. Delegación Álvaro Obregón. C.P. 01219. Tel: 5257-80-00, ext. 47063, 47064, Fax: 5269-27-01 y su página electrónica es**:** www.santander.com.mx

4.3.1.2 BBVA BANCOMER, S.A.

Grupo Financiero BBVA Bancomer (GFBB) es una institución financiera privada con importante presencia en México que ofrece una amplia variedad de productos y servicios financieros. Su principal actividad la realiza a través de BBVA Bancomer (el Banco), subsidiaria bancaria líder en México en términos de depósitos, cartera de crédito, número de cajeros automáticos y número de sucursales.

GFBB es una empresa controladora filial de Banco Bilbao Vizcaya Argentaria (BBVA), uno de los grupos financieros líderes en Europa y considerado entre uno de los más grandes de la Zona Euro. BBVA es un grupo financiero con una elevada solvencia y rentabilidad, tiene presencia en 31 países del mundo, destacando su compromiso con la región latinoamericana donde forma la franquicia financiera líder.

Se encuentra ubicada en Av. Universidad Núm. 1200 , Xoco. Distrito Federal. Delegación Benito Juárez.. C.P. 03339. Tel: 5621-6411 y su página electrónica es www.bancomer.com.mx

4.3.1.3 BANCO AUTOFIN MÉXICO, S.A.

El Banco Autofin México, S.A. tiene como misión ser el banco por excelencia de las familias mexicanas, permitiéndoles mejorar su economía presente y crear un futuro de mayor bienestar, diseñando oportunidades seguras, atractivas e innovadoras de ahorro y crédito.

Se encuentra ubicada en Av. Insurgentes Sur Núm.1235 Extremadura Insurgentes. Distrito Federal. Delegación Benito Juárez C.P 03740. Tel: 5063-28-00 y su página electrónica es www.bam.com.mx

4.3.1.4 BANCO AZTECA, S.A.

Banco Azteca es un banco joven perteneciente al Grupo Salinas que nació en octubre del 2002, ante la oportunidad derivada del bajo nivel de bancarización en México. El banco está orientado al sector de

menores ingresos, que representa un 70% de la población no atendida por los bancos tradicionales. Una gran ventaja desde el inicio de operaciones, fue la experiencia de más de 50 años de Grupo Elektra en el otorgamiento de crédito a dicho sector.

Se encuentra ubicada en Av. Ferrocarril de Río Frío Núm. 419-A10. Fracc. Industrial del Moral. Distrito Federal. Delegación Iztapalapa. C.P. 08500. Tel: 1720-70-00, Fax: 0155-8582-76-56 y su página electrónica es: www.bancoazteca.com.mx; email: salarcon@bancoazteca.com.mx

BANCO AZTECA®
Cambiamos la banca, cambia tú también

4.3.1.5 BANCO INBURSA, S.A.

Banco INBURSA es una empresa sólida dedicada desde hace más de 42 años al beneficio de sus clientes y lo demuestran ocupando actualmente el cuarto lugar en créditos comerciales del país. Ha creado importantes empresas especializadas, que unidas ofrecen buenos productos con el mejor servicio, cubriendo todas las necesidades financieras de sus clientes.

Asimismo, cuenta con Tarjeta de Crédito y Débito, Créditos Hipotecarios, Crédito Automotriz, Productos de Inversión y Fianzas, además de una extensa gama de Seguros de Vida, Gastos Médicos, Autos y Afore. Banco INBURSA cubre con enorme orgullo e integralmente las expectativas más exigentes de todos sus clientes, tanto personas físicas como morales.

Se encuentra ubicada en Av. Insurgentes Sur, Núm. 3500. Peña Pobre. Distrito Federal. Delegación Tlalpan. C.P 14060. Tel: 5325-05-05; 5325-04-77, Fax: 5325-05-25 y su página electrónica es: www.bancoinbursa.com.mx

INBURSA

4.3.1.6 BANCO NACIONAL DE MÉXICO, S.A.

En agosto de 2001, como resultado de la venta de Grupo Financiero Banamex-Accival a Grupo Financiero Citigroup, surge Grupo Financiero Banamex.

La incorporación a Citigroup le ha permitido ofrecer una extensa gama de servicios financieros en

México y el mundo, a través de sus empresas subsidiarias: Banamex, Acciones y Valores Banamex, Casa de Bolsa, Seguros Banamex y Afore Banamex.

Hoy en día, Banco Nacional de México es parte de la principal compañía de servicios financieros en el mundo, con 200 millones de cuentahabientes en más de 100 países.

Se encuentra ubicada en Isabel la Católica, Núm. 44 Centro Histórico. Distrito Federal. Delegación Cuauhtémoc. C.P 06000. Tel: 1226-63-63, Fax: 5225-46-72; su página electrónica es: www.banamex.com. y su email: leoherna@banamex.com

4.3.1.7 BANCO WAL-MART DE MÉXICO ADELANTE, S.A.

Banco Walt-Mart de México es un proveedor de servicios financieros para todos los clientes de las tiendas, clubes y restaurantes de Grupo Wal-Mart, a fin de contribuir a elevar su calidad de vida, apoyando al crecimiento del Grupo, la rentabilidad de sus accionistas y el crecimiento de sus asociados.

Se encuentra ubicada en José María Castorena, Núm. 470. San José de los Cedros. Distrito Federal. Delegación Cuajimalpa de Juárez. C.P. 05200. Tel: 2452-83-34; su página electrónica es: http://www.bancowalmart.com. Y su email: mhpelk@wal-mart.com

4.3.1.8 HSBC MÉXICO, S.A.

HSBC México, S.A. tiene como misión poner al alcance del deseo de sus clientes soluciones integrales a sus necesidades financieras, tales como: Cuentas Maestras, Cuentas de ahorro, Créditos e Inversiones.

Se encuentra ubicado en Av. Paseo de la Reforma, Núm. 347.Col. Cuauhtémoc. Delegación Cuauhtémoc. Distrito Federal. C.P. 06500. Tel: 01 (55) 5721 6600, Fax: 01 (55) 5721 2222; su página electrónica es: www.hsbc.com.mx y su email: alfonso.orozco@hsbc.com.mx

4.3.1.9 IXE BANCO, S.A.

Ixe mantiene como premisa fundamental el ofrecer a los clientes, productos y servicios de calidad que satisfagan sus necesidades financieras y que les den la seguridad, confianza y tranquilidad que se merecen.

Ixe desea estar cerca de sus clientes para asesorarlos en la elección de los instrumentos de ahorro, inversión y crédito que les garanticen un mejor futuro, y para apoyarlos en llevar a cabo sus proyectos financieros.

Se encuentra ubicado en Av. Paseo de la Reforma Núm. 505, Piso 48 .Col. Cuauhtémoc. Delegación Cuauhtémoc. Distrito Federal. C.P. 06500. Tel: 5268-90-00 su página electrónica es: www.ixe.com.mx y su email: magarzon@ixe.com.mx

4.3.1.10 BANCO DEL AHORRO NACIONAL Y SERVICIOS FINANCIEROS, S.N.C.

Es un institución bancaria de tipo Banca de Desarrollo cuya misión tiene por objeto apoyar el desarrollo institucional del sector de ahorro y crédito popular y promover la cultura financiera y el ahorro entre sus integrantes, a través de la oferta de productos y servicios adecuados, una sólida infraestructura tecnológica, un equipo humano profesional y comprometido, así como de la coordinación de apoyos del gobierno federal y de diversos organismos.

Se encuentra ubicado en Río Magdalena, Núm. 115. Col. Pueblo de Tizapán. Distrito Federal. Delegación Álvaro Obregón. C.P. 01090. Tel: 5481-33-00, Fax: 5481-33-22 y su página electrónica es: www.bansefi.gob.mx

4.3.1.11 BANCO NACIONAL DEL EJÉRCITO, FUERZA AÉREA Y ARMADA, S.N.C.

El 15 de Julio de 1947 inició operaciones el Banco Nacional del Ejército, Fuerza Aérea y Armada, bajo la figura jurídica de una Sociedad Anónima de Capital Variable. El Banco ha evolucionado a la par del desarrollo experimentado por el Sistema Financiero Mexicano y actualmente se organiza bajo la figura de las denominadas Sociedades Nacionales de Crédito, Instituciones de Banca de Desarrollo que forman parte de la Administración Pública Federal, pero mantienen personalidad jurídica y patrimonio propios.

Ante el remolino de la modernidad al que nos enfrentamos día con día, es necesario evolucionar al mismo ritmo que marca el tiempo, es por ello que el Banco Nacional del Ejército, Fuerza Aérea y Armada S.N.C., se posiciona en el punto estratégico avanzando a paso firme para brindar a sus clientes un servicio eficiente, seguro y práctico, manteniéndose de esta manera siempre a la vanguardia.

El Banco Nacional del Ejército, Fuerza Aérea y Armada, S.N.C. (Banjercito), conforme a su Ley Orgánica tiene como objetivo prioritario el proporcionar el servicio de banca y crédito a un sector estratégico de la Sociedad Mexicana: los miembros del Ejército, Fuerza Aérea y Armada de México.

Se encuentra ubicado Av. Industria Militar, No. 1055, 1er. Piso Col. Lomas de Sotelo 11200 México, D.F.; sus teléfonos son Conm. 5557 9188 ext. 2441; su página electrónica es: www.banjercito.com.mx y su correo electrónico: info@banjercito.com.mx

4.3.1.12 NACIONAL FINANCIERA, S.N.C.

NAFINSA tiene como misión promover el acceso de las MIPYMES a los servicios financieros; impulsar el desarrollo de proyectos sustentables y estratégicos para el país; promover el desarrollo del mercado de

valores y fungir como Agente Financiero del Gobierno Federal, con el fin de contribuir al crecimiento regional y a la creación de empleos.

Se encuentra ubicada en Insurgentes Sur, No. 1971. Col. Guadalupe Inn, C.P 01020, México, D.F.; su teléfono es: Conm. 5325 6000 y su página electrónica es: http://www.nafin.com

4.4 DELIMITACIÓN DE LA MUESTRA

De acuerdo con la unidad de análisis propuesta, se buscará el acceso para la aplicación del instrumento en cada una de las entidades financieras que la integran y que a su vez se definirán los estratos y el porcentaje de participación de cada uno de ellos.

CRITERIOS DE INCLUSIÓN

Las Instituciones de Banca Múltiple y de Banca de Desarrollo mexicanas localizadas en el Distrito Federal, cuyo sector se abocó al ámbito financiero, que se encuentran delimitadas en la unidad de análisis y que además están registradas en el Padrón de Identidades Financieras Supervisadas por la Comisión Nacional Bancaria y de Valores (CNBV).

CRITERIOS DE EXCLUSIÓN

Las Instituciones mexicanas dentro del sector financiero cuyo padrón de identidad se dedique a Grupos Financieros, Bursátiles, Sociedades de Inversión, Organizaciones y Actividades Auxiliares del Crédito, Entidades de Ahorro y Crédito popular, así como empresas que prestan Servicio a Entidades Financieras.

4.5 OPERACIONALIZACIÓN DE LAS VARIABLES Y DISEÑO DEL INSTRUMENTO PARA LA OBTENCIÓN DE DATOS

4.5.1 IDENTIFICACIÓN, DEFINICIÓN, OBJETIVO Y OPERACIONALIZACIÓN DE VARIABLES

Las variables que a continuación se enuncian son desplegadas de acuerdo a su rubro:

4.5.1.1 VARIABLES INDEPENDIENTES

Las variables independientes son las siguientes:

IDENTIFICACIÓN DE VARIABLES	DEFINICIÓN	INDICADORES (ITEMS)	OBJETIVO
DEMOGRÁFICAS			
X_1 = Edad	Edad en años cumplidos	Métrica de edad (intervalos de edad) 1= De 18 a 25 años 2= De 26 a 35 años 3= De 36 a 45 años 4= De 46 a 60 años 5= 61 años o más	Identificar la edad con la que cuenta el encuestado
X_2 = Sexo	Género del personal	1= Femenino 2= Masculino	Identificar el género del encuestado
X_3 = Nivel Jerárquico	Nivel de acuerdo al grado que ocupa cada empleado acorde al diagrama organizacional. Se entiende como nivel jerárquico al agrupamiento de puestos de trabajo, de acuerdo a la naturaleza general de funciones, responsabilidades y	1= Directivo 2= Gerencial 3= Ejecutivo 4= Operativo	Identificar el nivel jerárquico en el que se desenvuelve el encuestado.

IDENTIFICACIÓN DE VARIABLES	DEFINICIÓN	INDICADORES (ITEMS)	OBJETIVO
	complejidad de operaciones.[23]	5= Secretarial	
X_4= Tiempo laborando en la Institución	Tiempo de servicio en la institución financiera	Métrica de tiempo de servicio (intervalos de tiempo) 1= De 0 a 3 años 2= De 4 a 8 años 3= De 9 a 15 años 4= De 16 a 20 años 5= De 21 a 30 años 6= De 31 a 40 años 7= más de 40 años	Identificar el lapso de servicio que ha bridado el encuestado a la empresa.
X_5= Último grado de estudios terminados	Grado máximo de estudios terminado por los empleados	1= Técnico 2= Licenciatura 3= Maestría 4= Doctorado	Identificar el máximo grado de estudios que tiene el perfil del encuestado.
CONCEPTO			
X_1= Uso habilitado de redes sociales en	Si el empleado tiene habilitado el uso de redes sociales en el equipo que le fue proporcionado para realizar sus	1= Si 2= No	Saber si la institución tiene la opción de acceso a páginas que

[23] Ciemencia Jaime (1982). Diferencias Motivacionales según el nivel jerárquico en entidades financieras de servicio. *Revista Latinoamericana de Psicología*. 14(1).

IDENTIFICACIÓN DE VARIABLES	DEFINICIÓN	INDICADORES (ITEMS)	OBJETIVO
el trabajo	actividades diarias en la empresa.		aluden a las redes sociales.
X_2= Frecuencia de uso de redes sociales	Si el usuario acostumbra a hacer uso de la redes sociales en su vida diaria	1= Diario 2= Cada tercer día 3= Cada semana 4= Una vez al mes	Saber la frecuencia con la que el encuestado acostumbra a utilizar las redes sociales para conocer la susceptibilidad que el empleado tiene respecto a un ataque de Ingeniería Social.
X_3= Personas a las que se les revela información confidencial	Fuentes en las que el empleado suele divulgar información de tipo laboral.	1= Me guardo la nueva noticia 2= Se lo cuento a mis amigos 3= Se lo cuento a mi familia 4= Se lo cuento a mis compañeros de otros departamentos 5= Lo publico en mi muro de mi facebook 6= Lo publico en twitter 7= Lo coloco en el mensaje principal de mi messenger	Identificar hacia qué entidades el encuestado publica la información que acontece en su entorno laboral.
X_4= Abstenimiento de revelar información laboral	Revelación de información, por parte del empleado, de índole laboral hacia fuentes externas.	1= Les dice en donde labora 2= Les dice qué es lo que hace en su trabajo 3= Trata de cambiar el tema 4= Les responde con una pregunta 5= Evade la pregunta que le hicieron 6= Otro : _____	Identificar la susceptibilidad del encuestado para revelar información clasificada referente a su ámbito laboral.
X_5= Medios de comunicación	Medios que emplea el encuestado para	1= Intranet	Identificar aquellos medios de

IDENTIFICACIÓN DE VARIABLES	DEFINICIÓN	INDICADORES (ITEMS)	OBJETIVO
utilizados	comunicarse con sus compañeros de trabajo	2= Correo electrónico 3= Messenger 4= Personalmente 5= Escritos impresos 6= Otro : _____	comunicación que emplean los encuestados para comunicarse, en su ámbito laboral, con la finalidad de conocer la susceptibilidad que tienen los datos que viajan a través de la red.
X_6= Cuentas de correo utilizadas	Tipo de cuentas de correo utilizada en el trabajo del empleado para poder transferir documentos.	1= Cuenta interna proporcionada por la institución 2= Cuenta comercial como google, yahoo, Hotmail, etcétera	Identificar las medidas de seguridad, en cuanto a correo electrónico se refiere, para la protección de la información que viaja a través de la red.
X_7= Tipo de Messenger usado en el trabajo	Tipo de messenger que el empleado utiliza en tu trabajo.	1= Messenger Windows live 2= Google talk 3= Skype 4= Yahoo messenger 5= Pidgin 6= Kmess 7= Kopete 8= Meebo 9= Ebuddy 10= Tmsnc 11= Monkeymessenger 12= Movil Messenger	Saber si se emplea un cifrado predeterminado en la transferencia de datos a través de la red, en las comunicaciones entabladas por los encuestados.

IDENTIFICACIÓN DE VARIABLES	DEFINICIÓN	INDICADORES (ITEMS)	OBJETIVO
		13= Talkdroid 14= Ebuddy mobile 15= Msn Droid 16= Windows Live Messenger Mobile 17= NImbuzz 18= Ninguno 19= Otro : _____	
X_8= Temas que se hablan con los demás	Temas que el empleado acostumbra a charlar con sus compañeros de la empresa en donde labora.	1= Personales 2= Laborales con compañeros de mi área 3= Laborales con compañeros de otros departamento de la empresa 4= Laborales con amigos o compañeros que laboran en otras empresas del mismo giro 5= Inconformidades suscitadas en el trabajo	Identificar el tipo de información que es divulgada por parte de los encuestados en su ámbito laboral
X_{9A}= Medios de comunicación utilizados para transferir información (información de nuevos servicios de la empresa)	Medios de comunicación utilizados por los empleados, con mayor frecuencia, para la difusión de la información confidencial de nuevos servicios, dentro de la institución, hacia sus colegas.	1= Correo electrónico corporativo 2= Correo electrónico comercial (gmail, Hotmail, yahoo, etcétera) 3= Usando la intranet 4= Messenger 5= Entrega impresa de manera personal 6= Otro : _____	Identificar los medios de comunicación empleados dentro del corporativo para enviar información de índole confidencial dentro de la institución.

IDENTIFICACIÓN DE VARIABLES	DEFINICIÓN	INDICADORES (ITEMS)	OBJETIVO
X_{9B}= Medios de comunicación utilizados para transferir información (información de proyectos de la empresa)	Medios de comunicación utilizados por los empleados, con mayor frecuencia, para la difusión de la información confidencial de proyectos, dentro de la institución, hacia sus colegas.	1= Correo electrónico corporativo 2= Correo electrónico comercial (gmail, Hotmail, yahoo, etcétera) 3= Usando la intranet 4= Messenger 5= Entrega impresa de manera personal 6= Otro : _____	Identificar los medios de comunicación empleados dentro del corporativo para enviar información de índole confidencial dentro de la institución.
X_{9C}= Medios de comunicación utilizados para transferir información (información de estudios de mercado de la empresa)	Medios de comunicación utilizados por los empleados, con mayor frecuencia, para la difusión de la información confidencial de estudios de mercado, dentro de la institución, hacia sus colegas.	1= Correo electrónico corporativo 2= Correo electrónico comercial (gmail, Hotmail, yahoo, etcétera) 3= Usando la intranet 4= Messenger 5= Entrega impresa de manera personal 6= Otro : _____	Identificar los medios de comunicación empleados dentro del corporativo para enviar información de índole confidencial dentro de la institución.
X_{9D}= Medios de comunicación utilizados para transferir información (información de reportes de actividades de la empresa)	Medios de comunicación utilizados por los empleados, con mayor frecuencia, para la difusión de la información confidencial de reportes de actividades, dentro de la institución, hacia sus colegas.	1= Correo electrónico corporativo 2= Correo electrónico comercial (gmail, Hotmail, yahoo, etcétera) 3= Usando la intranet 4= Messenger 5= Entrega impresa de manera personal 6= Otro : _____	Identificar los medios de comunicación empleados dentro del corporativo para enviar información de índole confidencial dentro de la institución.
X_{9E}= Medios de comunicación	Medios de comunicación utilizados por	1= Correo electrónico corporativo	Identificar los medios de comunicación

IDENTIFICACIÓN DE VARIABLES	DEFINICIÓN	INDICADORES (ITEMS)	OBJETIVO
utilizados para transferir información (información de nuevos productos de la empresa antes de que salgan al mercado)	los empleados, con mayor frecuencia, para la difusión de la información confidencial de nuevos productos antes de que salgan al mercado, dentro de la institución, hacia sus colegas.	2= Correo electrónico comercial (gmail, Hotmail, yahoo, etcétera) 3= Usando la intranet 4= Messenger 5= Entrega impresa de manera personal 6= Otro : _____	empleados dentro del corporativo para enviar información de índole confidencial dentro de la institución.
X_{9F}= Medios de comunicación utilizados para transferir información (información de servicios financieros de la empresa)	Medios de comunicación utilizados por los empleados, con mayor frecuencia, para la difusión de la información confidencial de servicios financieros, dentro de la institución, hacia sus colegas.	1= Correo electrónico corporativo 2= Correo electrónico comercial (gmail, Hotmail, yahoo, etcétera) 3= Usando la intranet 4= Messenger 5= Entrega impresa de manera personal 6= Otro : _____	Identificar los medios de comunicación empleados dentro del corporativo para enviar información de índole confidencial dentro de la institución.
X_{9G}= Medios de comunicación utilizados para transferir información (información de contratos de la empresa)	Medios de comunicación utilizados por los empleados, con mayor frecuencia, para la difusión de la información confidencial de contratos, dentro de la institución, hacia sus colegas.	1= Correo electrónico corporativo 2= Correo electrónico comercial (gmail, Hotmail, yahoo, etcétera) 3= Usando la intranet 4= Messenger 5= Entrega impresa de manera personal 6= Otro : _____	Identificar los medios de comunicación empleados dentro del corporativo para enviar información de índole confidencial dentro de la institución.
X_{10}= Frecuencia con la que escucha hablar del término de la Ingeniería Social	Frecuencia con la cual el empleado ha escuchado hablar del término de la Ingeniería Social	1= Ninguna 2= Poca 3= Regularmente	Saber si el encuestado conoce el término de la Ingeniería Social y sus efectos.

IDENTIFICACIÓN DE VARIABLES	DEFINICIÓN	INDICADORES (ITEMS)	OBJETIVO
		4= Muy Frecuentemente	
X_{11}= Uso de la Ingeniería Social	El empleado no sólo conoce el término del a Ingeniería Social, sino que también hace uso de la misma con fines laborales.	1= Si 2= No	Saber si el encuestado aplica la Ingeniería Social.
X_{12}= Nociones del ataque informático Pharming	Se desea saber si el empleado tiene nociones del ataque informático denominado Pharming, debido a que es uno de los ataques informáticos más comunes que se presentan con frecuencia en el sector financiero. Un ataque informático consiste en aprovechar alguna debilidad o falla (vulnerabilidad) en el software, en el hardware, e incluso, en las personas que forman parte de un ambiente Informático; a fin de obtener un beneficio, por lo general de índole económico, causando un efecto negativo en la seguridad del sistema, que luego repercute directamente en los activos de la organización.[24]	1= Nunca 4= Muy frecuentemente	Identificar si el encuestado tiene nociones referentes a en qué consiste el ataque informático especificado.
X_{13}= Nociones del ataque informático Phising	Se desea saber si el empleado tiene nociones del ataque informático denominado Phising, debido a que es uno de los ataques informáticos más comunes que se presentan con frecuencia en el sector financiero.	1= Desconocimiento 4= Conocimiento	Identificar si el encuestado tiene nociones referentes a en qué consiste el ataque informático especificado.

[24] Mieres, Jorge (2009). *Ataques Informáticos: Debilidades de Seguridad comúnmente explotadas*. Evil Fingers White paper.

IDENTIFICACIÓN DE VARIABLES	DEFINICIÓN	INDICADORES (ITEMS)	OBJETIVO
X_{14}= Frecuencia de cambio de contraseñas	La frecuencia con la que el empleado acostumbras a cambiar sus contraseñas de uso común.	1= Cada 3 meses 2= Cada 6 meses 3= Cada año 4= Cada año y medio 5= Siempre conservo la misma	Saber si en las políticas institucionales se incluye una cláusula en donde se exija el cambio de contraseña constante de los usuarios para la seguridad de la información contenida en los storage utilizados.
X_{15A}= Frecuencia para responder encuestas no corporativas (dentro de la institución)	Frecuencia con la que el empleado acostumbra a responder encuestas o cuestionarios, de índole no corporativo, dentro de la institución dónde labora	1= Nunca 4= Muy frecuentemente	Identificar la disposición que tiene los empleados de la institución para ser susceptibles a divulgar información de cualquier índole, por medio del llenado de encuestas o cuestionarios, dentro de la institución.
X_{15B}= Frecuencia para responder encuestas no corporativas (fuera de la institución)	Frecuencia con la que el empleado acostumbra a responder encuestas o cuestionarios, de índole no corporativo, fuera de la institución dónde labora	1= Nunca 4= Muy frecuentemente	Identificar la disposición que tiene los empleados de la institución para ser susceptibles a divulgar información de cualquier índole, por medio del llenado de encuestas o cuestionarios, fuera de la institución en donde labora.
X_{16}= Nivel de Seguridad de la Información con el que se estima	Nivel de seguridad de la información que estima el empleado tiene la empresa.	1= De 0% a 30% 2= De 31% a 50% 3= De 51% a 70%	Identificar el porcentaje perceptivo por parte del encuestado, que

IDENTIFICACIÓN DE VARIABLES	DEFINICIÓN	INDICADORES (ITEMS)	OBJETIVO
cuenta la organización.	Se entiende por **seguridad de la información** a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistema tecnológicos que permitan resguardar y proteger la información buscando mantener la *confidencialidad*, la *autenticidad* e *Integridad* de la misma. • DALTABUIT, Godás Enrique, *et al.*, *Seguridad de la información*. Ed. Limusa: Noriega, México, 2007.	4= De 71% a 90% 5= De 91% a 100%	tiene referente al nivel de seguridad de la información con el que cuenta la institución en la que labora.

4.5.1.2 VARIABLES DEPENDIENTES

La variable dependiente es la siguiente:

IDENTIFICACIÓN DE VARIABLES	DEFINICIÓN	INDICADORES (ITEMS)	OBJETIVO
Y_1= Impacto de la Ingeniería Social	Efecto o actuación que ejerce la Ingeniería Social entorno a la Seguridad de la información en las instituciones de Banca Múltiple y de Banca de Desarrollo del sector financiero. Se entiende por **seguridad de la información** a todas aquellas medidas preventivas y reactivas del hombre, de las organizaciones y de los sistema tecnológicos que permitan resguardar y proteger la información buscando mantener la *confidencialidad*, la *autenticidad* e *Integridad* de la misma. • DALTABUIT, Godás Enrique, *et al.*, *Seguridad de la información*. Ed. Limusa: Noriega, México, 2007.	1= Alto 2= Bajo	Estimar el impacto que tiene la Ingeniería Social en la Seguridad de la Información en las instituciones de Banca Múltiple y de Banca de Desarrollo del sector financiero.

4.6 INSTRUMENTO

El instrumento que se llevó a cabo para efectuar el estudio en cuestión fue una encuesta en línea presentada por medio de una página Web, con la finalidad, en primera instancia, de que los encuestados pudiesen interactuar con una ambiente visual y dinámico y, en segunda, para que el vaciado de datos fuese mucho más rápido y efectivo.

La difusión de dicha página hacia las entidades en estudio se realizó mediante un enlace *(link),* único para cada entidad, para que direccionara a los encuestados a la página electrónica correspondiente. Dicha liga fue abierta por cada uno de los entrevistados por medio de su navegador web a través de internet, para ello se requirió que las entidades financieras encuestadas tuviesen conexión a internet para contestar la encuesta. Con esto se pretendió determinar el nivel de cultura de seguridad de la información con el que cuentan las instituciones mexicanas de Banca Múltiple y de Banca de Desarrollo del Distrito Federal en el sector financiero.

Cabe destacar que por cuestiones confidenciales y de índole académico no se mostrará el nombre de la entidad financiera encuestada.

A continuación se presenta la imagen que permite visualizar la pagina web del cuestionario aplicado a los encuestados:

Instrumento aplicado por medio de una página web

Fig 42. Instrumento aplicado en la Investigación.

A continuación se enuncian cada una de las preguntas presentadas en la página Web con sus respectivas posibles respuestas:

La siguiente encuesta es realizada con fines académicos y sus respuestas son estrictamente confidenciales.

Objetivo: Conocer la Cultura de la Seguridad de la Información Organizacional

Muchas gracias por tomarse el tiempo para completar esta encuesta. Su participación es de gran importancia para dicha investigación. Esta encuesta requiere 3 minutos de su tiempo. Sus respuestas serán totalmente anónimas y con fines académicos.

Si tiene alguna duda nuestro correo es silaning@gmail.com

Instrucciones: Selecciones una opción dando click sobre ésta. Únicamente en el caso en el que se le indique podrá seleccionar más de una respuesta.

Edad: *

- De 18 a 25 años
- De 26 a 35 años
- De 36 a 45 años
- De 46 a 60 años
- 61 años o más

Sexo: *

Femenino
- Femenino
- Masculino

Nivel Jerárquico: *

Directivo
- Directivo
- Gerencial
- Ejecutivo
- Operativo
- Secretarial

Tiempo laborando en la Institución: *

De 0 a 3 años
- De 0 a 3 años
- De 4 a 8 años
- De 9 a 15 años
- De 16 a 20 años
- De 21 a 30 años
- De 31 a 40 años
- más de 40 años

Último grado de estudios terminados: *

- Técnico
- Licenciatura
- Maestría
- Doctorado

1. ¿Tiene habilitado el uso de redes sociales (facebook, linkedin, myspace, hi5) en su equipo de oficina? *

- Si
- No

2. ¿Con qué frecuencia hace uso de las redes sociales en su vida diaria?

- Diario
- Cada tercer día
- Cada semana
- Una vez al mes

A partir de aquí puede seleccionar más de una respuesta

3. Supongamos que lo han comisionado como líder de un proyecto de suma importancia para la empresa, está muy emocionado(a) y gustoso(a) de que lo hayan elegido, ¿Qué haría inmediatamente después de que le den la noticia? *

- [ ] Me guardo la nueva noticia
- [ ] Se lo cuento a mis amigos
- [ ] Se lo cuento a mi familia
- [ ] Se lo cuento a mis compañeros de otros departamentos
- [ ] Lo publico en mi muro de mi facebook
- [ ] Lo publico en twitter
- [ ] Lo coloco en el mensaje principal de mi messenger

4. Imagine que asiste a una reunión en la cual le presentan a nuevas personas, está muy contento(a) y comienza a conocerlos, de pronto le preguntan sobre su trabajo, usted: *

- [ ] Les dice en donde labora
- [ ] Les dice qué es lo que hace en su trabajo
- [ ] Trata de cambiar el tema
- [ ] Les responde con una pregunta
- [ ] Evade la pregunta que le hicieron
- [ ] Other:

5. ¿Por qué medios suele comunicarse con sus compañeros? *

- [ ] Intranet
- [ ] Correo electrónico
- [ ] Messenger
- [ ] Personalmente
- [ ] Escritos impresos
- [ ] Other:

6. ¿Qué tipo de cuentas de correo electrónico utiliza en su trabajo para tansferencia de archivos? *

- [ ] Cuenta interna proporcionada por la institución
- [ ] Cuenta comercial como google, yahoo, Hotmail, etcétera

7. ¿Qué tipo de messenger utiliza en su trabajo? *

- [ ] Messenger Windows live
- [ ] Google talk
- [ ] Skype
- [ ] Yahoo messenger
- [ ] Pidgin
- [ ] Kmess
- [ ] Kopete
- [ ] Meebo
- [ ] Ebuddy
- [ ] Tmsnc
- [ ] Monkeymessenger
- [ ] Movil Messenger
- [ ] Talkdroid
- [ ] Ebuddy mobile
- [ ] Msn Droid
- [ ] Windows Live Messenger Mobile
- [ ] Nimbuzz
- [ ] Ninguno
- [ ] Other:

8. ¿Qué temas acostumbra a charlar con sus compañeros de la empresa en donde labora? *

- [ ] Personales
- [ ] Laborales con compañeros de mi área
- [ ] Laborales con compañeros de otros departamento en la empresa
- [ ] Laborales con amigos o compañeros que laboran en otras empresas del mismo giro
- [ ] Inconformidades suscitadas en el trabajo

Para la siguiente pregunta responda cada uno de los incisos

9. Por qué medio(s) transmite regularmente a sus jefes, compañeros o personal a su cargo:

a) La información de nuevos servicios de la empresa *

- [ ] Correo electrónico corporativo
- [ ] Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- [ ] Usando la intranet
- [ ] Messenger
- [ ] Entrega impresa de manera personal
- [ ] Other:

b) La información de proyectos de la empresa *

- [ ] Correo electrónico corporativo
- [ ] Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- [ ] Usando la intranet
- [ ] Messenger
- [ ] Entrega impresa de manera personal
- [ ] Other:

c) La información de estudios de mercado de la empresa *

- [ ] Correo electrónico corporativo
- [ ] Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- [ ] Usando la intranet
- [ ] Messenger
- [ ] Entrega impresa de manera personal
- [ ] Other:

d) La información de reportes de actividades de la empresa *

- [ ] Correo electrónico corporativo
- [ ] Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- [ ] Usando la intranet
- [ ] Messenger
- [ ] Entrega impresa de manera personal
- [ ] Other:

e) La información de nuevos productos antes de que salgan al mercado *

- [ ] Correo electrónico corporativo
- [ ] Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- [ ] Usando la intranet
- [ ] Messenger
- [ ] Entrega impresa de manera personal
- [ ] Other:

f) La información de servicios financieros *

- [ ] Correo electrónico corporativo
- [ ] Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- [ ] Usando la intranet
- [ ] Messenger
- [ ] Entrega impresa de manera personal
- [ ] Other:

g) Información respecto a contratos *

- [ ] Correo electrónico corporativo
- [ ] Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- [ ] Usando la intranet
- [ ] Messenger
- [ ] Entrega impresa de manera personal
- [ ] Other:

Par las siguientes preguntas seleccione sólo una opción

10. ¿Con qué frecuencia ha escuchado el término de la Ingeniería Social? *

Ninguna
- Ninguna
- Poca
- Regularmente
- Muy Frecuentemente

11. ¿Utiliza la Ingeniería Social? *

- Si
- No

12. En una escala del 1 al 4 ¿Con qué frecuencia se han experimentado ataques de tipo Pharming en su organización? *

El pharming es una modalidad de ataque informático, que consiste en suplantar al Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el propósito de conducirte a una página Web falsa.

	1	2	3	4	
Nunca	○	○	○	○	Muy frecuentemente

13. En una escala del 1 al 4 ¿Qué tanto conocimiento tiene acerca del ataque de tipo Phising en su organización? *

	1	2	3	4	
Desconocimiento	○	○	○	○	Conocimiento

14. ¿Con qué frecuencia acostumbra a cambiar sus contraseñas? *

- Cada 3 meses
- Cada 6 meses
- Cada año
- Cada año y medio
- Siempre conservo la misma

En una escala del 1 al 4,

15. ¿Con qué frecuencia responde encuestas o cuestionarios que no sean corporativos:?

a) Dentro de la institución

	1	2	3	4	
Nunca	○	○	○	○	Muy frecuentemente

b) Fuera de la institución

	1	2	3	4	
Nunca	○	○	○	○	Muy frecuentemente

16. ¿Con qué porcentaje de seguridad de la información estima que cuenta su organización? *

De 0% a 30%	De 31% a 50%	De 51% a 70%	De 71% a 90%	De 91% a 100%
○	○	○	○	○

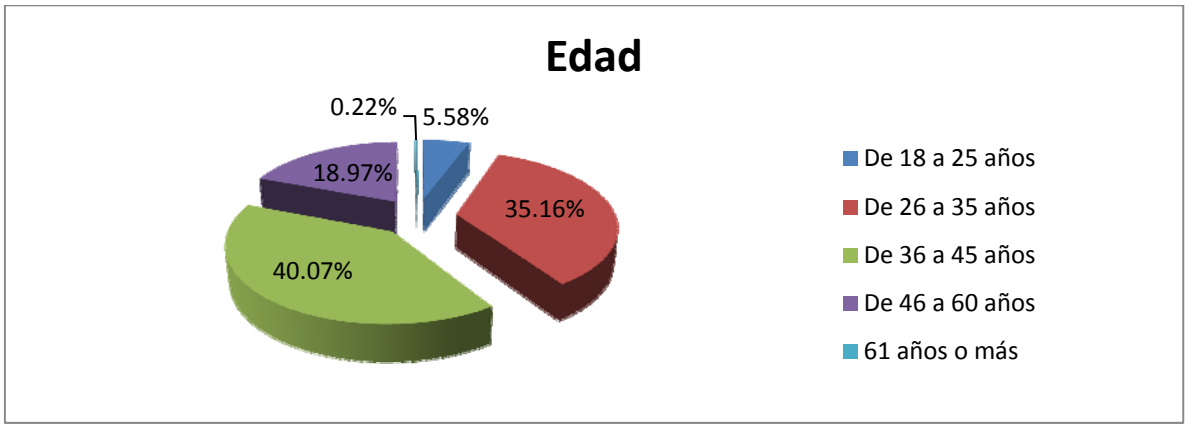
GRACIAS

V. RESULTADOS

Los resultados se reflejan en dos apartados; el primero de ellos aborda la descripción de los datos demográficos por medio de estadísticas a base de gráficas y, el segundo apartado, contiene un gráfico de porcentajes por cada pregunta de la encuesta aplicada. Cabe señalar que la muestra requerida a cada institución bancaria fue del 10% de su población de empleados.

Los resultados se enuncian a continuación:

5.1 DATOS DEMOGRÁFICOS

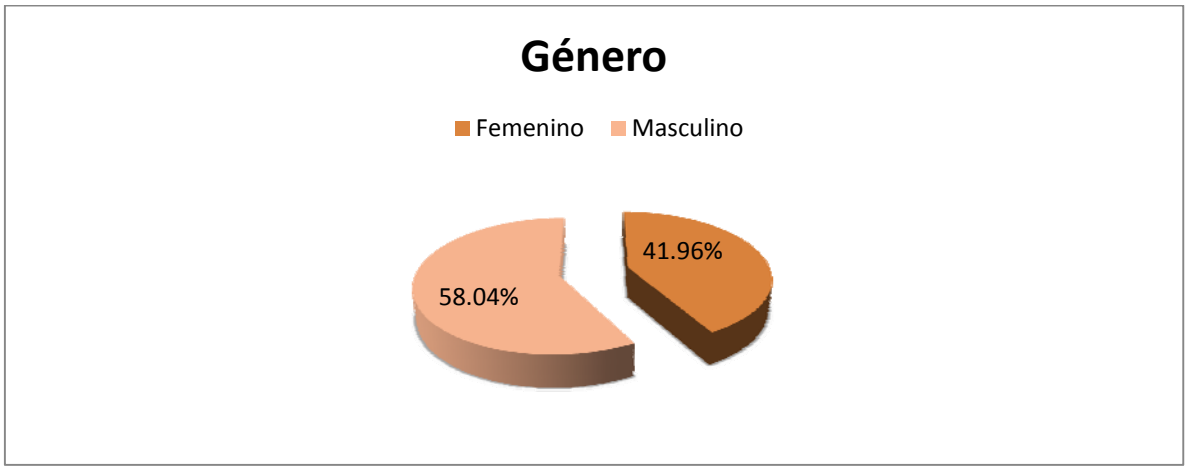


Interpretación: Como se puede observar en el gráfico, el rango de edad sobresaliente de los trabajadores de las instituciones financieras, con un 40.07%, es de 36 a 45 años; de éste le sigue, en segundo lugar, el 35.16% de los trabajadores con un rango de edad de 26 a 35 años y en tercer lugar se posiciona con un 18.97% el rango de edad entre 46 y 60 años.

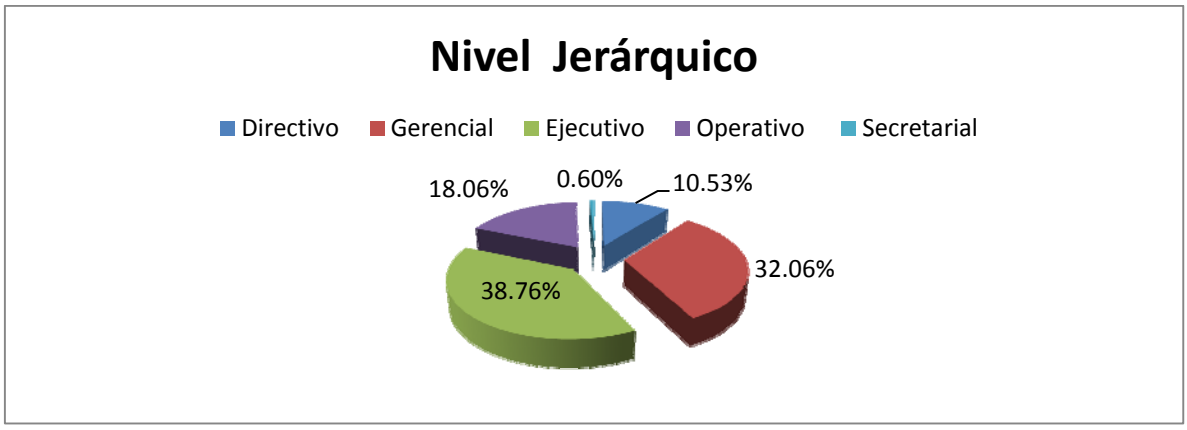
De dicha información se puede destacar que el sector financiero cuenta con un amplio número de trabajadores cuyas edades oscilan entre los 36 y 45 años de edad, lo que permite asimila que mayoritariamente el perfil de las personas que ocupan una plaza en el ámbito financiero, alude a personas de edad media. Sin embargo, el 5.58% de los encuestados pertenecientes al rango de edad de los 18 a 25 años, así como de los trabajadores mayores a los 61 años cuyo porcentaje ocupa un 0.22% del total de los encuestados, reflejan un menor índice de contratación; esto puede deberse a que la instituciones financieras probablemente tengan establecidas políticas de contratación de personal que cumpla con estatutos específicos tal como la contratación de personal titulado. Por otro lado, se sabe que la edad promedio para concluir una carrera profesional es de los 21 a los 25 años de edad, según el tipo de carrera profesional a la que se haga alusión, para fines del sector en análisis, las carreras afines que podrían intervenir en dicho ámbito serían: Contabilidad, Administración, Economía, Ingeniería en Computación, Informática o carreras afines, así como Psicología y Derecho.

De dichas carreras se tiene conocimiento, según planes de estudio de escuelas públicas, que la duración de las mismas para la conclusión de estudios es de 4 a 5 años promedio, mientras que en escuelas particulares la duración es de 3 años, por lo que los encuestados que respondieron que sus edades oscilan en el rango de los 18 a los 25 años de edad se encuentran posiblemente estudiando y trabajando. Como se puede observar en el gráfico, la población de los trabajadores cuyas edades oscilan entre los 18 y 25 años de edad representa muy posiblemente a los trabajadores que se encuentran concluyendo sus estudios, por lo que el índice de contratación de los mismos es escaso. Por otra parte, para el dato reflejado con respecto a una menor incidencia de empleados activos mayores a 61 años, se puede deducir que esto puede deberse a que la mayoría optó por la jubilación.

Asimismo, podemos observar que un poco más de la cuarta parte de los encuestados son jóvenes recién egresados y con una fidelidad laboral aproximada de 0 a 4 años (según el análisis de las subsecuentes gráficas), sin embargo, las instituciones financieras abren las puertas a dicha generación y ponen todo de su parte para creer en las habilidades de dichos aspirantes. Esto habla muy bien del sector financiero, ya que brinda la oportunidad a jóvenes entusiastas que buscan poner en práctica sus conocimientos adquiridos en su educación superior y que de acuerdo con los datos posteriores cumplen con una fidelidad constante hacia la institución.

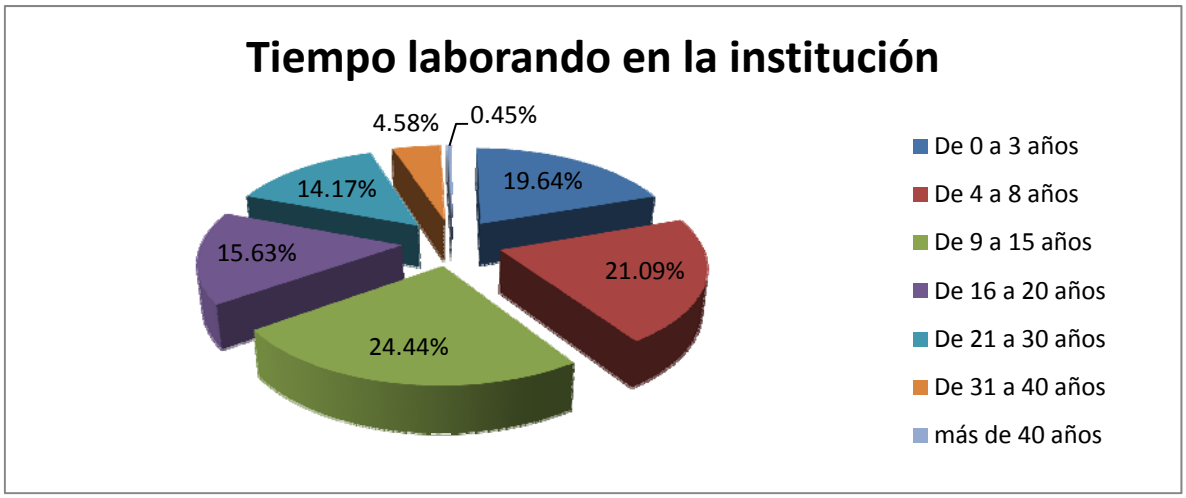


Interpretación: Del gráfico podemos observar que un 58.04% de la población pertenecen al género masculino, mientras que un 41.96% son de género femenino. De tales resultados se puede destacar que la población de trabajadores que tiene una mayor presencia en el ámbito financiero son los caballeros, debido a que ocupan más de la mitad de los empleos otorgados por las entidades financieras. La diferencia en porcentaje entre estos dos géneros es del 16.08%, porcentaje considerado medianamente alto debido a que refleja un poco más de la décima parte del total de los encuestados, y del cual se puede percibir una remarcada y menor incidencia, del género femenino, en el ámbito laboral financiero.



Interpretación: Se observa que el nivel Ejecutivo encabeza la lista de los niveles jerárquicos con un 38.76% de la población encuestada, el segundo lugar lo ocupan los niveles Gerenciales con un 32.06%, mientras que en el tercer lugar se posiciona el nivel Operativo con un 18.06% y a éste le sigue el nivel Directivo con un 10.53%. Como se puede visualizar en el gráfico el nivel jerárquico que tuvo una menor incidencia en la participación de la encuesta fue el Secretarial, el cual se refleja con un 0.60% del total de los encuestados.

Tales datos manifiestan que en el sector financiero labora un porcentaje alto del personal cuyas plazas pertenecen al nivel ejecutivo, mientras que el nivel jerárquico que menor participación tiene en dicho sector, en cuanto a vacantes ocupadas, es el nivel secretarial.



Interpretación: Del gráfico podemos observar que un 24.44% del personal que se encuentra laborando en el sector financiero tiene un lapso de fidelidad a las organizaciones financieras de 9 a 15 años; el segundo lugar lo ocupan los trabajadores que tienen una antigüedad de 4 a 8 años en cumplimiento de su labor, periodo que se ve reflejado con un 21.09%; mientras que en tercer lugar se posiciona el lapso de antigüedad de 0 a 3 años representando un 19.64%; y el 4°, 5° y 6° lugar lo ocupan las antigüedades, por parte de los

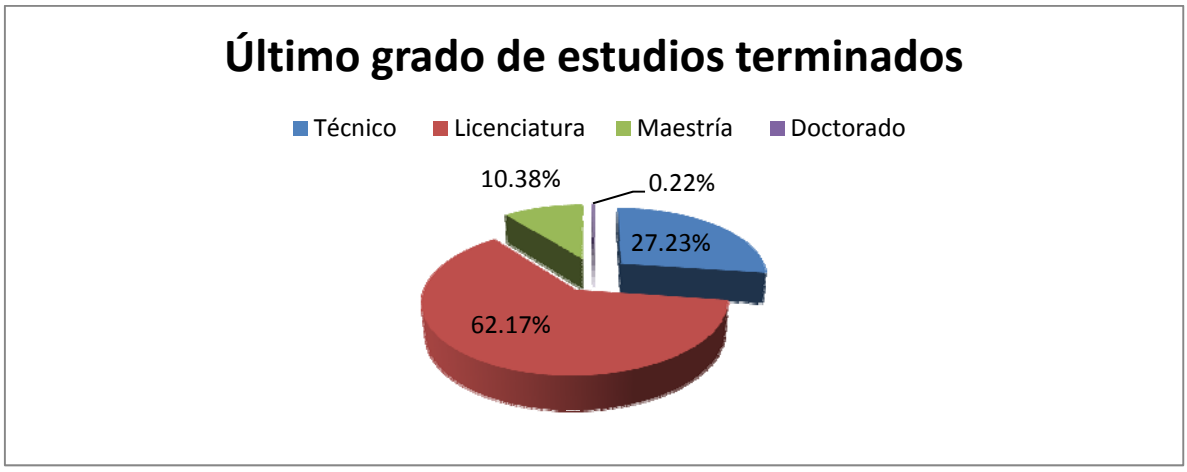
trabajadores que se encuentra laborando dentro del sector financiero, los periodos de 16 a 20 años, de 21 a 30 años y de 31 a 40 años respectivamente.

Asimismo, de dichas estadísticas se puede inferir que existe una menor presencia del personal del sector financiero cuyas edades exceden los 50 años, ya que la antigüedad laboral que menor presencia tiene en la gráfica oscila de los 41 años en adelante, hecho que puede considerarse debido a las jubilaciones de los empleados, o bien a la recesión de contratos por parte de las organizaciones financieras a los interesados.

Por otro lado, se puede visualizar la existencia de un número mayoritario de trabajadores cuya antigüedad oscila de los 4 a 15 años de labor en el sector financiero, lo que implica que la fidelidad de los trabajadores al sector financiero es amplia y esto es una labor reconocida por su gran desempeño a cada una de las instituciones que lo conforman, debido a que las instituciones propician un ambiente en el que personal se siente partícipe de la organización, no como un miembro más, sino como un integrante elemental de la misma.

Finalmente, cabe resaltar que existe un porcentaje alto que alude al 19.64% de los encuestados los cuales cuentan con una antigüedad de 0 a 3 años de labor a la institución financiera, lo que permite que el análisis se vierta en dos interpretaciones. La primera de ellas implica que el sector financiero está dispuesto a recibir a personal nuevo o recién egresado de sus carreras, que se encuentre calificado para ocupar un empleo en alguna de sus instituciones y la razón por la cual existe un índice bajo de años de fidelidad a las instituciones financieras es debido a ello. Por otro lado, la segunda interpretación, que se encuentra estrechamente ligada con la primera podría implicar que la fidelidad existente por parte de los trabajadores hacia su institución laborar es escasa, ya que puede existir una continua rotación de personal o contrataciones por servicios profesionales de periodos cortos, tal y como lo observamos en el gráfico al visualizar la antigüedad.

Cabe destacar que tomando en consideración la última interpretación, este hecho es preocupante, ya que representa el 3er. lugar del total de los encuestados y podría implicar una baja fidelidad por parte de los trabajadores hacia las instituciones correspondientes, lo que traería como consecuencia, en la mayoría de los casos, una mala actitud por parte de los empleados, reflejándose en el decremento del desempeño y rendimiento profesional de los mismos al no sentirse identificados y partícipes de manera plena con la empresa a la que pertenecen.



Interpretación: Como se puede observar en el gráfico, existe un mayor número de empleados que cubren un perfil de Licenciatura; éste se ve reflejado con un 62.17% que implica un poco más de la mitad de los encuestados. Así mismo en segundo lugar se posicionan, con un 27.23% el personal cuyo perfil académico es de nivel Técnico y en tercer lugar aparecen, con un 10.38% reflejando un poco más de la décima parte de la población encuestada, empleados cuya educación abarca nivel Maestría.

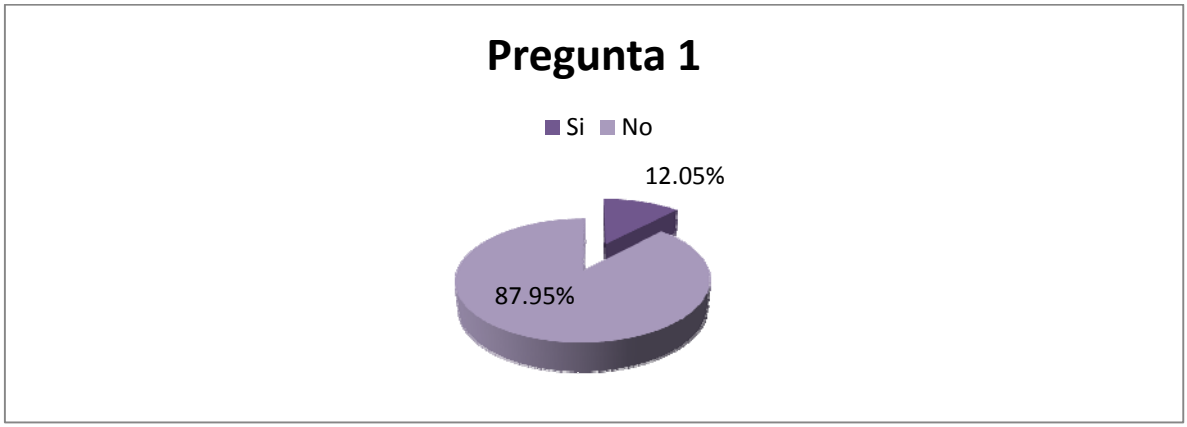
Por otro lado, el menor índice de nivel de estudios que se observa se ve reflejado en el nivel de grado de Doctorado, sin embargo, no se descarta dicha posibilidad ya que tiene un porcentaje de 0.22%.

De dichas estadísticas se puede deducir que el nivel de grado de estudios que funge mayoritariamente en el perfil de los empleados de las organizaciones del sector financiero es Licenciatura y subsecuentemente niveles Técnicos. De ello se observa la coherencia que existe entre la antigüedad de los trabajadores y sus edades debido a que los datos arrojados reflejan que existe un mayor número de trabajadores cuyas edades oscilan en el rango 26 a 35 años de edad, edad promedio en la que los estudiantes se gradúan y comienzan su estancia laboral. De igual manera, se observa un menor porcentaje de incidencia de trabajadores que cuentan con un nivel de estudios Técnico y éstos se comparan con la población de trabajadores cuyas edades oscilan entre los 18 y 25 años de edad que representan un 5.58% de la población total, lo que implica que los empleados de este rango de edades posiblemente cuenta con un nivel de estudios técnico al igual que otros tantos empleados cuyas edades podrían oscilar en los otros rangos propuestos para dicho estudio, lo que permitiría completar el 27.23% que representa el total de los empleados que dijo tener carrea Técnica. Esto sin considerar que probablemente los empleados dentro del rango de los 18 a 25 años de edad (el que representa el 5.58% de los encuestados) podrían ya tener el grado de Licenciatura.

5.2 DATOS ESTADÍSTICOS POR PREGUNTA

1. ¿Tiene habilitado el uso de redes sociales (facebook, linkedin, myspace, hi5) en su equipo de oficina? *

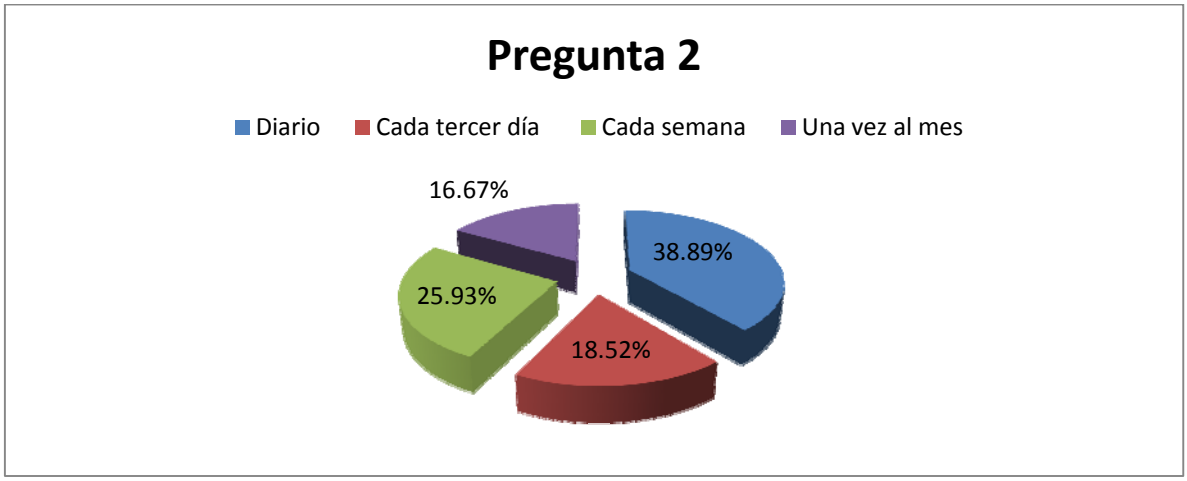
- Si
- No



Interpretación: Se puede visualizar en el gráfico que de la respuesta a la pregunta 1 con el objetivo de conocer si las instituciones financieras tienen habilitado el uso de las redes sociales en sus estaciones de trabajo, la respuesta con mayor frecuencia fue "No", respuesta que generó un porcentaje del 87.95%, mientras que el otro 12.05% restante respondió que "Si" tiene habilitado el uso de dichas redes sociales. Cabe destacar que el hecho de tener habilitadas las página web de redes sociales como Facebook, Linkedin, Myspace, hi5, Twitter entre otras, no implica que esto sea malo, sin embargo, si no se tienen nociones respecto a una cultura de seguridad de la información, el uso indebido de dichas redes sociales podrían representar puntos vulnerables para la institución, aunque esto depende del tipo de información que se publica, lo cual se analizará en las preguntas posteriores. Es importante señalar que al mencionar "uso indebido" se alude a que el usuario, en este caso los trabajadores de las instituciones financieras, publiquen información relacionada con su persona y la vinculación que tienen con la institución financiera o bien simplemente información sensible referente a la institución en la que laboran.

2. ¿Con qué frecuencia hace uso de las redes sociales en su vida diaria?

- Diario
- Cada tercer día
- Cada semana
- Una vez al mes



Interpretación: En relación con la pregunta número 2 respecto a conocer la frecuencia de uso de las redes sociales por parte de los empleados de la institución en su vida diaria, cabe señalar que dicha pregunta tiene estrecha relación con la anterior debido a que sólo el 12.05% de la población encuestada respondió afirmativamente a la pregunta 1 y, únicamente de éste porcentaje, que refleja un poco más de la décima parte de la población de empleados, el 38.89% de los encuestados respondió que utiliza diariamente el uso de redes sociales; en segundo lugar se posicionan, con un 25.93%, las personas que consultan las redes sociales cada semana; en tercer lugar se colocan los trabajadores que consultan dichas páginas cada tercer día y le siguen cercanamente aquellos empleados que las consultan una vez al mes con un 18.52% y 16.67% respectivamente.

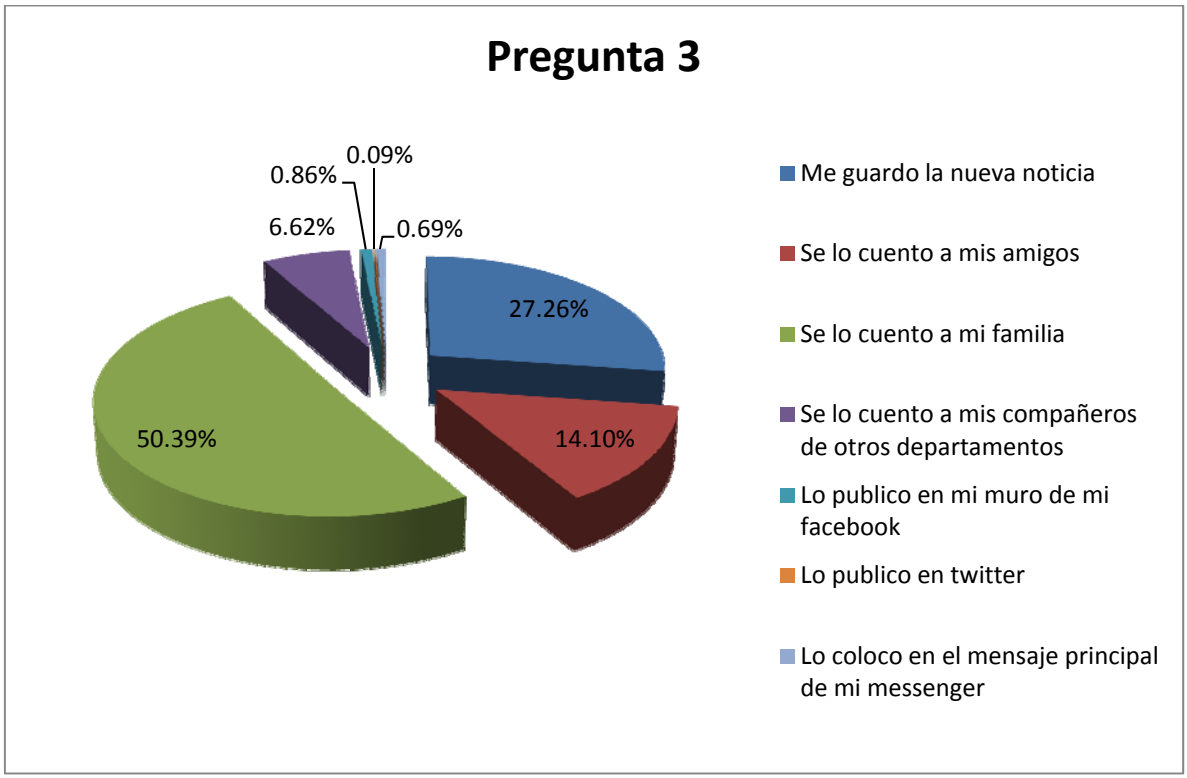
De dichos resultados cabe resaltar que le uso diario de redes sociales señala que las personas que consultan diariamente, o cada tercer día sus redes sociales, tienen mayor probabilidad de comunicar las actividades cotidianas que acontecen a su alrededor, a diferencia de personas que frecuentan el uso de las mismas cada semana o una vez al mes. Sin embargo, no se descarta aún la posibilidad de que a sabiendas de que se efectúa un uso diario de las redes sociales por parte de los empleados, éstos no carezcan de una cultura de seguridad de la información que se ve reflejada en el uso de las redes sociales que manejan. Dicho supuesto se irá esclareciendo conforme al avance del análisis de las siguientes preguntas.

A partir de las siguientes preguntas las respuestas proporcionadas por los empleados de las instituciones financieras pudieron ser múltiples, es decir, cada empleado pudo responde más de una respuesta; por lo que el número de frecuencias presentadas en cada una de las tablas excede el total de encuestados que representan el 10% de la población de empleados.

A partir de aquí puede seleccionar más de una respuesta

3. Supongamos que lo han comisionado como líder de un proyecto de suma importancia para la empresa, está muy emocionado(a) y gustoso(a) de que lo hayan elegido, ¿Qué haría inmediatamente después de que le den la noticia? *

- [ ] Me guardo la nueva noticia
- [ ] Se lo cuento a mis amigos
- [ ] Se lo cuento a mi familia
- [ ] Se lo cuento a mis compañeros de otros departamentos
- [ ] Lo publico en mi muro de mi facebook
- [ ] Lo publico en twitter
- [ ] Lo coloco en el mensaje principal de mi messenger



Interpretación: Respecto a dicha pregunta se planteó una situación común con la que el empleado se sintiera identificado para que posteriormente respondiera la respuesta o respuestas acorde a las acciones que tomaría inmediatamente después de recibir una noticia laboral, esto con la finalidad de detectar a quién o a quiénes el empleado divulga parte de los acontecimientos ocurridos en su trabajo, obteniendo lo siguiente:

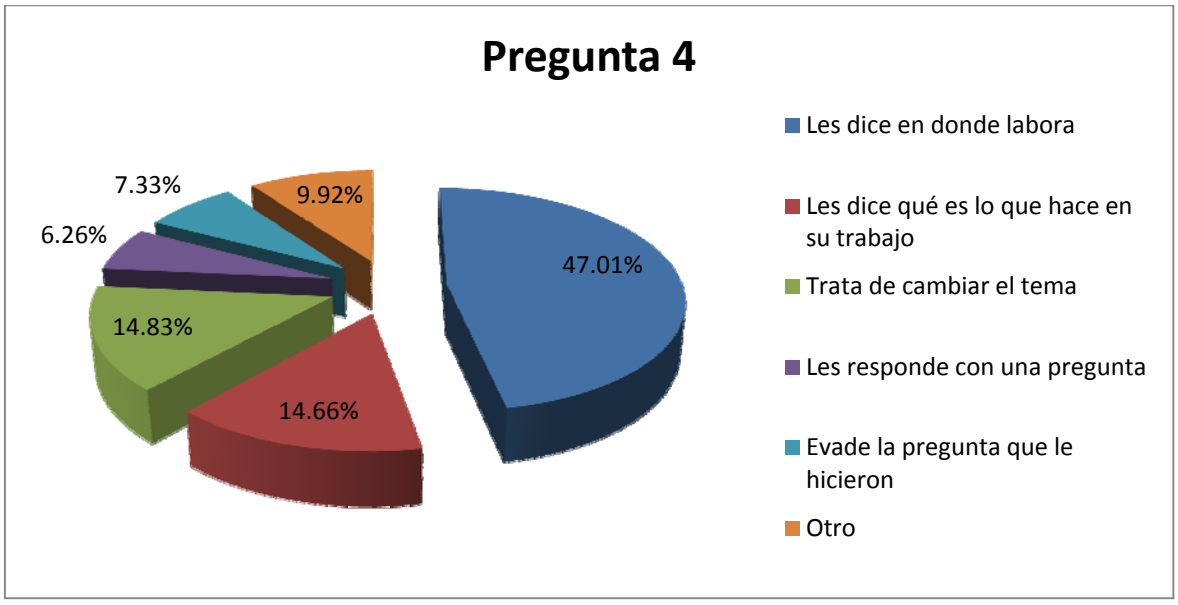
El 50.39% respondió que cuenta la noticia a sus familia, en segundo lugar con un 27.26% contestó que acostumbra guardarse la nueva noticia, mientras que, posicionando en tercer lugar, el 14.10% de los empleados respondió que se lo cuenta a sus amigos. Asimismo, el 6.62% respondió que cuenta la noticia a

sus compañeros que laboran en otros departamentos, lo que puede implicar fuga de información entre áreas, sería recomendable verificar las políticas de la organización y cotejarlas con éste punto ya que las pequeñas fugas de información confidencial, aunque se presenten dentro de la misma institución, pueden generar predisposición por parte de los otros empleados o bien que dicha información se extienda a áreas externas.

Por otro lado, el restante 1.64% de los encuestados (5°, 6° y 7° lugar) lo componen respuestas que aluden a que el empleado acostumbra a publicar la noticia en su muro de Facebook, en Twitter y/o como leyenda del mensaje principal de su messenger. En este punto es importante resaltar que tal porcentaje de empleados carecen de una cultura de seguridad de la información, y éste suceso podría propiciar fugas de información relevantes. Asimismo, cabe destacar que el hecho de hacer publicaciones de éste tipo no necesariamente implican un peligro para la organización, sin embargo, pueden representar pequeñas goteras de fugas de información que acumuladas podrían constituir un punto vulnerable para las instituciones del sector financiero. Aunque un 1.64% de la población encuestada no representa un peligro extremo para la institución, es recomendable fomentar en los empleados la abstinencia de publicar noticias de manera meticulosa respecto a los acontecimientos derivados de la institución en la que se labora.

4. Imagine que asiste a una reunión en la cual le presentan a nuevas personas, está muy contento(a) y comienza a conocerlos, de pronto le preguntan sobre su trabajo, usted: *

- ☐ Les dice en donde labora
- ☐ Les dice qué es lo que hace en su trabajo
- ☐ Trata de cambiar el tema
- ☐ Les responde con una pregunta
- ☐ Evade la pregunta que le hicieron
- ☐ Other:



Interpretación: En dicha pregunta se planteó una situación en la que comúnmente existe el intercambio de información entre amigos, conocidos y desconocidos respecto a temas laborales, familiares, y de cualquier

otra índole; con el objetivo de conocer la información que proporcionan los empleados a desconocidos (nuevas personas por conocer) en reuniones como fiestas, convivios, cumpleaños, bodas, XV años, entre otras; se planteó la pregunta correspondiente, obteniendo lo siguientes resultados:

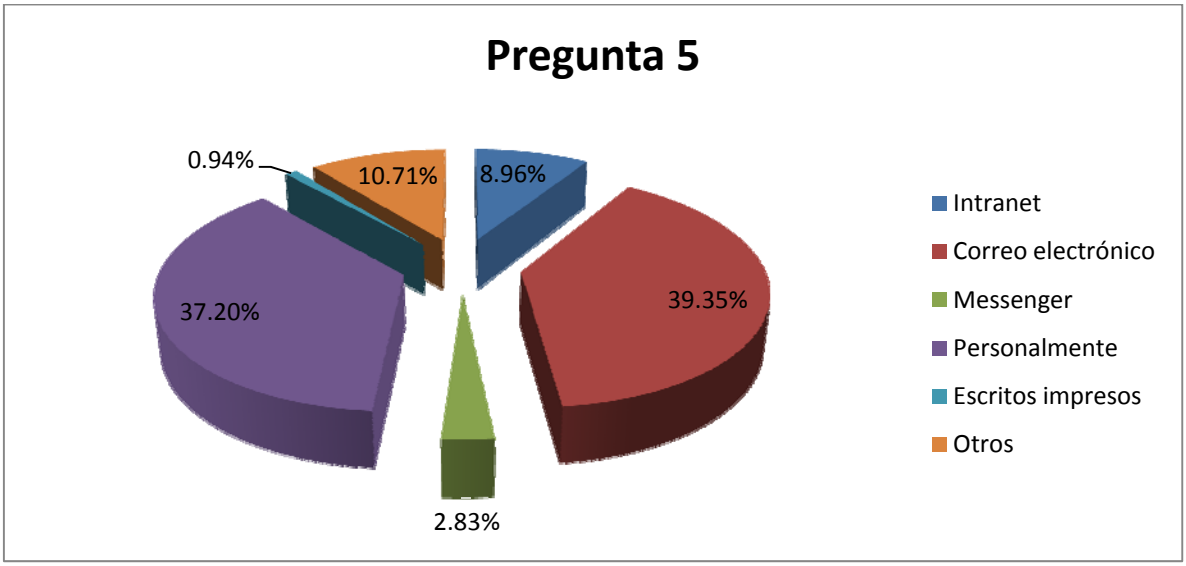
El 47.01% respondió que acostumbra a comentarles a nuevos conocidos el lugar en donde labora, es decir, les dice el nombre de la institución en la que labora. En segundo lugar, con un 14.83% se posicionan los empleados que al presentarse ante esta situación ratan de cambiar el tema; subsecuentemente en tercer lugar se ubican con un 14.66% los empleados que divulgan las actividades que realizan en su trabajo; como se puede observar el segundo y tercer lugar de las respuestas proporcionadas por los empleados tienen un porcentaje similar con una diferencia mínima del 0.17%, de lo cual se puede interpretar que las respuesta de "Les dice qué es lo hace en su trabajo" y "Trata de cambiar el tema" fueron muy frecuentes y a la par con las respuestas de los encuestados, ya que casi empatan. Asimismo, en cuarto lugar con un 9.92% se ubican respuestas distintas que fueron opcionales como respuesta abierta colocándola en el rubro de nombre "Otros", cabe señalar que en dichas respuestas se encuentran las siguientes: No dan detalles, diplomáticamente reservan información, no divulgan ni funciones ni actividades, no dan explicaciones, trata de intercambiar ideas, trata de vender productos, dicen que les gusta lo que hacen, realizan promoción al banco, mienten, no comentan que trabajan en el ámbito financiero, bromean, no comentan el nombre de la empresa, toman en consideración a qué persona se le revelará la información, no informan nada, comentan en dónde laboran y el puesto que ocupan sin detallar actividades, dicen su profesión sin dar detalles adicionales, buscan el motivo que generó la pregunta, o bien no acostumbran a revelar datos de su persona con desconocidos.

De dichos datos podemos destacar que el 14.66% de los encuestados representa una porción significativa y al comentarle a nuevas personas que se desconocen, las labores que realiza el empleado en su trabajo, pueden ser un foco rojo de alerta para la institución financiera, sin embargo, el decir qué actividades se realizan en la institución de manera global puede generar pequeñas fugas de información confidencial que en conjunto podrían representar una gran vulnerabilidad.

Por otra parte, se puede observar que el 7.33% de los empleados evade la pregunta que le hacen respecto a su ámbito laboral y el otro 6.26% responden con otra pregunta, lo que implica que en ambos casos los empleados evaden las preguntas generadas por desconocidos respecto a su trabajo. Cabe resaltar que esta es una buena técnica para reservarse la información que podría recaer en el ámbito confidencial y evitar con ello fugas de información que representen un peligro para la institución financiera o bien para el mismo personal.

5. ¿Por qué medios suele comunicarse con sus compañeros? *

- [ ] Intranet
- [ ] Correo electrónico
- [ ] Messenger
- [ ] Personalmente
- [ ] Escritos impresos
- [ ] Other:



Interpretación: Con respecto a la pregunta 5 se pretendió conocer los medios por los cuales existe una comunicación constante entre empleados, para ello se colocaron una serie de posibles respuestas de múltiple selección, es decir, un empleado pudo responder más de una opción; esto con la finalidad de conocer el medio principal de comunicación utilizado con mayor frecuencia por los trabajadores de la institución, de dichos resultados se obtuvo lo siguiente.

En primer lugar, se posiciona con un 39.35% el correo electrónico (institucional o comercial), medio primordial que utilizan los empleados para comunicarse entre ellos; en segundo lugar resalta con un 37.20% la respuesta que alude a que los empleados se comunican con sus compañeros de manera personal; en tercer lugar sobresale con un 10.71% la opción seleccionada de "Otros" la cual en su mayoría incorpora como respuesta que su medio de comunicación principal es por medio del teléfono, el celular, mensajes de texto, Microsoft Office Communicator, la aplicación Whats App, el Inbox de Facebok, así como canales internos de la institución.

Asimismo, en cuarto lugar con un 8.96% se coloca el rubro del uso de intranet como medio principal de comunicación, el 2.83% aseguró utilizar el Messenger y el 0.94% restante respondió que lo hace a través de escritos impresos.

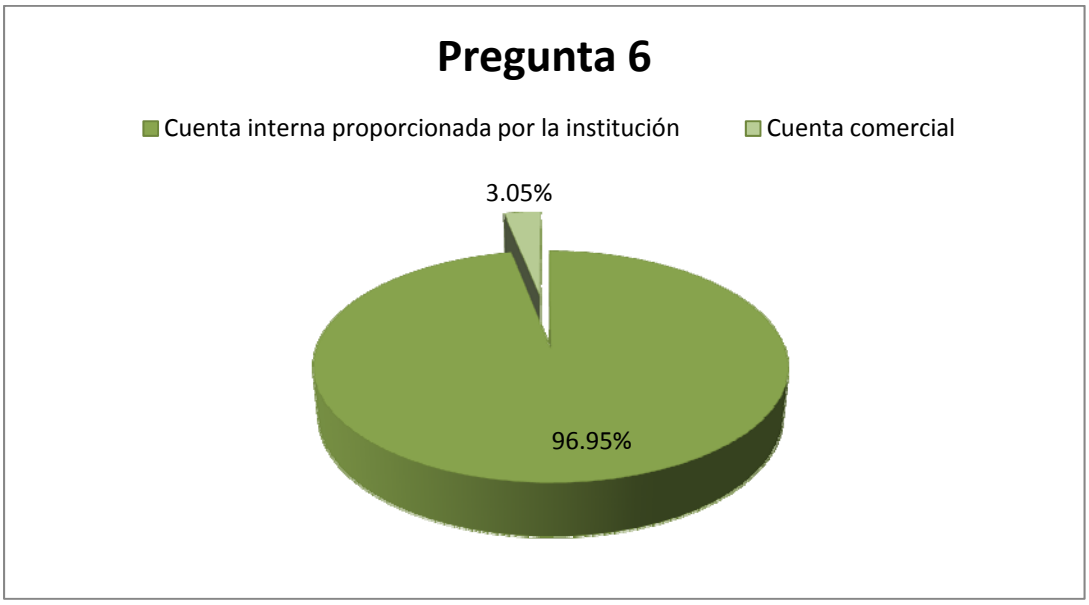
De dichos resultados se puede señalar que aludiendo a los tres primeros lugares, el tipo de comunicación empleado por los trabajadores es común y no representa una alerta significativa para la institución; sin embargo, es recomendable que cuando los empelados se comuniquen de manera personal entre ellos,

busquen el medio adecuado para hacerlo (oficina, sala de reunión, etcétera) ya que puede existir la posibilidad de que terceras personas se enteren de instrucciones o información de índole confidencial. Asimismo, el uso de correo electrónico facilita la comunicación constante entre los colegas, sin embargo se recomienda emplear un servidor de correo que cuente con un protocolo de comunicación de tipo SSL (Secure Socket Layer), el cual proporciona un canal seguro y confiable por el cual la información viajará de manera segura evitando con ello que un tercero pueda extraer dicha información a través de herramientas como los Sniffer. Al igual para el rubro de "otros", en el que se implican el envío de mensajes de texto y llamadas telefónicas, así como el messenger de las redes sociales como facebook, es recomendable que las instituciones financieras aseguren que no exista intervención de línea telefónica o en su defecto hacer del conocimiento de los empleados que la información que comuniquen a través de la línea telefónica, los mensajes de texto o los messsenger de las redes sociales, no sean de índole confidencial

Finalmente, con respecto a los últimos tres lugares, se puede destacar un reconocimiento a las instituciones financieras debido a que sus empleados hacen un uso de una intranet que permite el paso de información de manera interna. Por otra parte, en lo que respecta a los escritos impresos, se recomienda que el personal tenga cuidado al momento de enviar a imprimir dichos documentos debido a que la información que en estos se plasme puede ser sensitiva y por consiguiente podrían ser considerados como puntos cruciales para la fuga de información dentro de la institución. Asimismo, cabe resaltar que el uso de Messenger para comunicarse con sus compañeros de trabajo no implica un fallo de seguridad, simplemente se recomienda implementar aplicaciones tal como "Simp Lite" que permite que la información viaje de manera cifrada a través de la red, o bien mensajeros que ya contengan un mecanismo de cifrado tal como Skype.

6. ¿Qué tipo de cuentas de correo electrónico utiliza en su trabajo para tansferencia de archivos? *

- ☐ Cuenta interna proporcionada por la institución
- ☐ Cuenta comercial como google, yahoo, Hotmail, etcétera



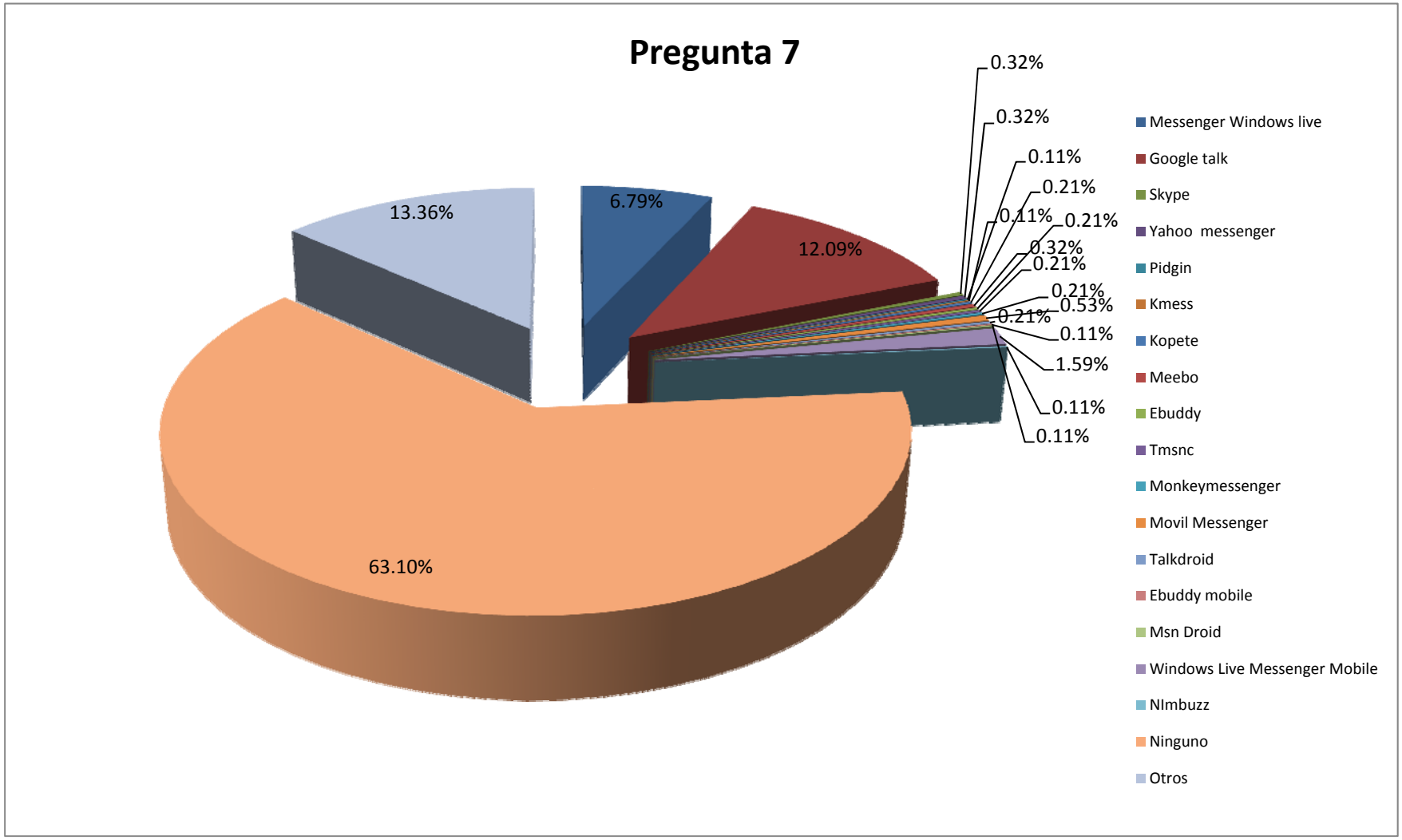
Interpretación: La pregunta 6 se realizó con la finalidad de conocer el tipo de cuenta de correo que utilizan los empleados dentro de la institución, cabe señalar que se planteó la posibilidad de que cada empleado pudiera responder 2 respuestas como máximo y una como mínimo. Los resultados obtenidos fueron los siguientes.

Con un 96.95% los empleados respondieron que utilizan la cuenta interna proporcionada por la institución, hecho que favorece la seguridad de las instituciones bancarias debido a que se cuenta con un servidor de correo específico para la institución, el cual se recomienda haga uso de protocolos de seguridad de tipo SSL (Secure Socket Layer) para asegurar que la información que viaja a través de la red lo haga de manera segura y cifrada.

Por otro lado, se observa que únicamente el 3.05% restante del total de los encuestados respondió que hace uso de una cuenta comercial. Con respecto de esta información cabe señalar que el uso de correo electrónico comercial no implica que se atente contra la seguridad de la información de las instituciones financieras; sin embargo, es de vital importancia hacer mención que la mayoría de los servidores comerciales que proporcionan cuentas gratuitas tienen un contrato de acuerdo previo con el usuario, el cual establece que al momento que el usuario se registra para obtener los beneficios de éste servicio, está obligado a firmar declarando que toda la información almacenada en su correo personal, permanecerá en las bases de datos de éstas compañías. Este aspecto puede ser un punto vulnerable para la divulgación de información confidencial de las instituciones del sector financiero, por ello se recomienda hacer uso continuo de la cuenta interna proporciona por la institución, únicamente para fines laborales, al momento de adjuntar archivos con información sensible de la institución o bien al transmitir instrucciones a colega respecto a proyectos o aspectos laborales. Para situaciones fuera del ámbito laboral si se recomienda el uso de las cuentas comerciales; sin embargo, es importante señalar a los empleados que tengan consciencia del tipo de información que transmitirán a través de dicha vía de comunicación.

7. ¿Qué tipo de messenger utiliza en su trabajo? *

- [ ] Messenger Windows live
- [ ] Google talk
- [ ] Skype
- [ ] Yahoo messenger
- [ ] Pidgin
- [ ] Kmess
- [ ] Kopete
- [ ] Meebo
- [ ] Ebuddy
- [ ] Tmsnc
- [ ] Monkeymessenger
- [ ] Movil Messenger
- [ ] Talkdroid
- [ ] Ebuddy mobile
- [ ] Msn Droid
- [ ] Windows Live Messenger Mobile
- [ ] Nimbuzz
- [ ] Ninguno
- [ ] Other:


Pregunta 7
0.32%
0.32%
0.11%
0.21%
0.11%
0.21%
0.32%
0.21%
0.21%
0.53%
0.21%
0.11%
1.59%
0.11%
0.11%
6.79%
12.09%
13.36%
63.10%
Messenger Windows live
Google talk
Skype
Yahoo messenger
Pidgin
Kmess
Kopete
Meebo
Ebuddy
Tmsnc
Monkeymessenger
Movil Messenger
Talkdroid
Ebuddy mobile
Msn Droid
Windows Live Messenger Mobile
NImbuzz
Ninguno
Otros

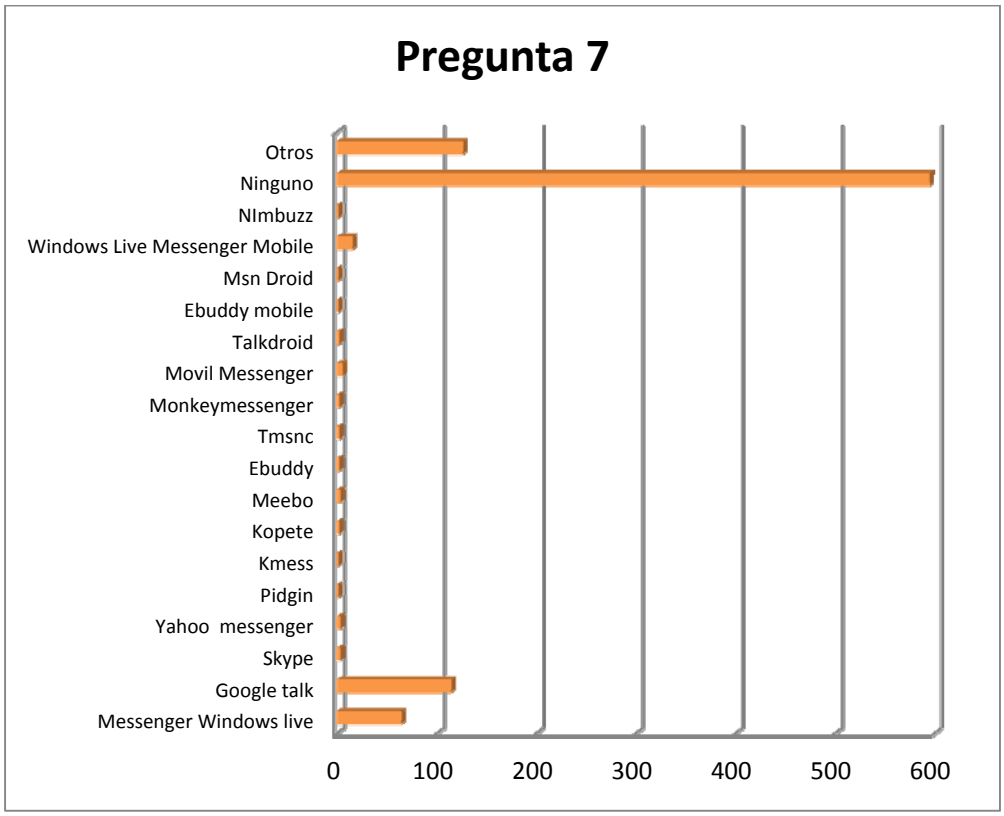
Interpretación: El objetivo de dicha pregunta fue conocer el tipo de Messenger que se utiliza con mayor frecuencia dentro de las instituciones financieras, cabe señalar que un empleado pudo elegir entre 19 posibles opciones, de las cuales la última fue abierta para que los empleados colocaran otra opción alternativa. A sabiendas de que en la pregunta número 5 se supo que únicamente el 2.83% de los encuestados respondió que utiliza como medio de comunicación principal el Messenger. Los resultados en cuanto al tipo de Messenger que se utiliza dentro de la institución por parte de los trabajadores que representa el 2.83% de los encuestados, fueron los siguientes.

En primer lugar se posiciona con un 63.10% los empleados que a pesar de contar con dicha aplicación dentro de la institución no la utilizan, en segundo lugar se encuentra con un 13.36% "otro" tipo de Messenger especificado por los trabajadores de las instituciones financieras, dichas aplicación se mencionan a continuación: GroupWise o Novell Group, Mensajería Web, a través de su celular con aplicaciones tal como BBMSN (Black Berry Messenger), gwa.b-enlinea (Novell Web Access), Microsoft Office Communicator, Thomson Reuters Messenger, HP MyRoom (mensajero de HP), BigAnt y WhatsApp, Google Talk, viber y what´s up Messenger msn (iphone). De estas opciones que pertenecen al rubro de "otros" cabe señalar que varios empleados indicaron desconocer el tipo de aplicación utilizada, otros hicieron mención de navegadores web e incluso del uso de correos electrónicos personales. De dicha información se puede inferir que existe una población significativa que desconoce determinadas tecnologías de la información como lo es el Messenger y para mitigar ésta falta de cultura respecto a TICs se recomienda fomentar conferencias, cursos o platicas referentes al uso de aplicaciones que funciona como medios de comunicación síncrona y asíncrona, sobre todo a las generaciones de rangos de edades mayores a los 45 años.

El tercer lugar del ranking de la pregunta en cuestión lo obtiene, con un 12.09%, el mensajero de Google Talk, la cual es una aplicación que no consume mucha memoria en el equipo de trabajo y que facilita el intercambio de ideas entre compañeros; sin embargo, cabe aclarar que Google advierte que en la actualidad no realiza ningún trabajo de cifrado en los chats o las llamadas de voz, pero anuncia que el cifrado de las conversaciones estará listo para cuando el producto supere la fase de pruebas y sea lanzada una versión estable, por lo que para dicho uso se recomienda implementar aplicaciones extras que permitan el cifrado de la información que viaja a través de la red, una opción viable podría ser el uso de Simp Lite, aplicación que permite cifrar conversaciones de cualquier mensajero de manera gratuita.

Asimismo, se puede observar que el 6.79% de la población utiliza en su trabajo el Messenger Windows Live, mientras que el otro 4.68% restante, se reparte entre aplicaciones menos comunes como Kopete, Yahoo, Pidgin, entre otros. Sin embargo, cabe señalar que dentro del sector financiero del Distrito Federal, de acuerdo a los resultados arrojados, se hace uso de aplicaciones de mensajería instantánea instaladas en los celulares de los empleados, dichas aplicaciones señalan ser Movil Messenger, Talkdroid, Ebuddy mobile, Msn Droid entre otros dependiendo de la marca y sistema operativo del celular. Así mismo dentro de éste 4.68% entran la mención de interfaces a través de la web como Meebo y Ebuddy que permiten dicha comunicación. Ante estos datos es importante aclarar que el uso del Messenger no es malo como comúnmente se cree, sin embargo, como ya se planteó anteriormente se recomienda el uso de aplicaciones que cifren la información que se transmite a través de la red, sobre todo en las estaciones de trabajo así como dispositivos celulares.

A continuación se muestra un gráfico de barras que muestra con mayor claridad el tipo de Messenger que más se utiliza en las instituciones financieras:

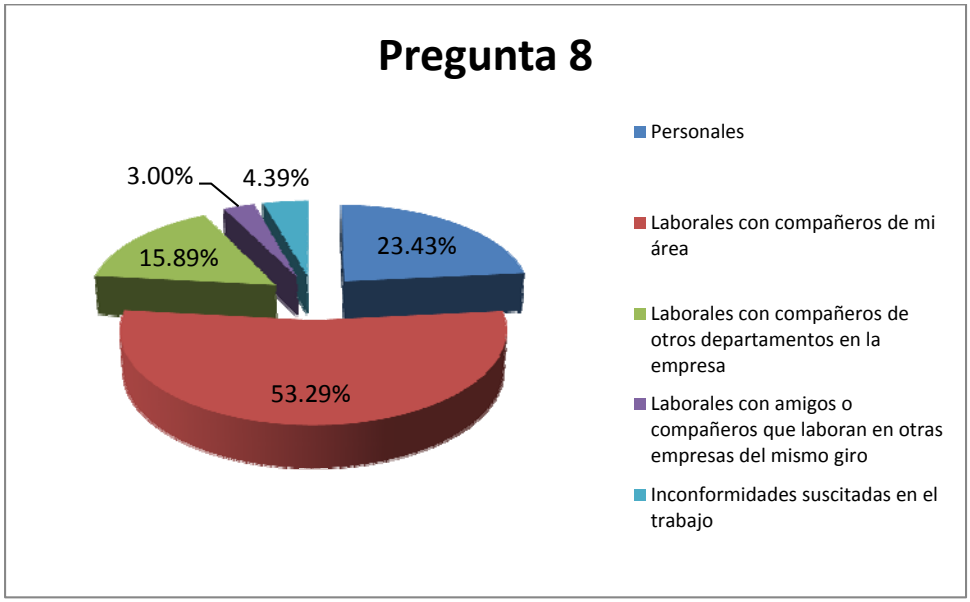


Interpretación: Como se puede observar, el primer lugar lo encabezan los encuestados que respondieron que no hacen uso de éste tipo de aplicaciones, en segundo lugar se posicionan otros tipos de Messenger utilizados por los empleados y que ya se especificaron en la interpretación anterior.

Posteriormente, en tercer lugar se coloca el uso del mensajero de Google, el llamado "Google talk", y finalmente, en cuarto lugar se encuentra el uso del común, pero no menos importante, "Messenger Windows Live". Asimismo, en el gráfico se puede visualizar que el uso de aplicaciones de tipo Messenger para celulares también sobresale; sin embargo, su presencia es menor.

8. ¿Qué temas acostumbra a charlar con sus compañeros de la empresa en donde labora? *

- [ ] Personales
- [ ] Laborales con compañeros de mi área
- [ ] Laborales con compañeros de otros departamento en la empresa
- [ ] Laborales con amigos o compañeros que laboran en otras empresas del mismo giro
- [ ] Inconformidades suscitadas en el trabajo



Interpretación: Con dicha pregunta se buscó conocer los temas de conversación que los miembros del sector financiero acostumbran a entablar entre ellos, obteniendo los siguientes resultados:

El 53.29% de los encuestados aseguró que charla temas laborales con sus compañeros de área, el 23.43% señaló que expresa comúnmente sus problemas personales; en tercer lugar se ubica con un 15.89% las conversaciones acerca de temas laborales con compañeros de otros departamentos dentro de la institución financiera, un 4.39% asegura que sus temas de conversación son acerca de inconformidades suscitadas en el trabajo; y el 3.00% restante expresa que comenta temas laborares con amigos o compañeros que trabajan en otras empresas del mismo giro.

De los datos anteriores se pude concluir que existe un amplio índice de confidencialidad debido a que las charlas entabladas por los empleados de las instituciones financieras, con sus mismos compañeros de área, son normales y suelen suscitarse a menudo. Por otra parte, existe un índice elevado que corresponde al 15.89% de los encuestados en el que se señala que conversan temas laborales con compañeros de otros departamentos dentro del a institución, lo que podría genera fugas de información sensitiva a través de otras áreas. Asimismo, existe un índice considerable en cuanto a la expresión de inconformidades suscitadas en el trabajo, esto implicaría que dicho porcentaje de empleados pueda ser susceptible de inhibir su compromiso con la institución en la que labora, por lo que se recomienda que se haga un estudio en donde se reflejen las causas primordiales que suscitan dicha reacción y se realice algo al respecto; esto es importante debido a que si el empleado no se siente identificado como parte elemental de la organización

podría tomar represalias en contra de la misma o bien permitir la fuga de información sensitiva de la empresa.

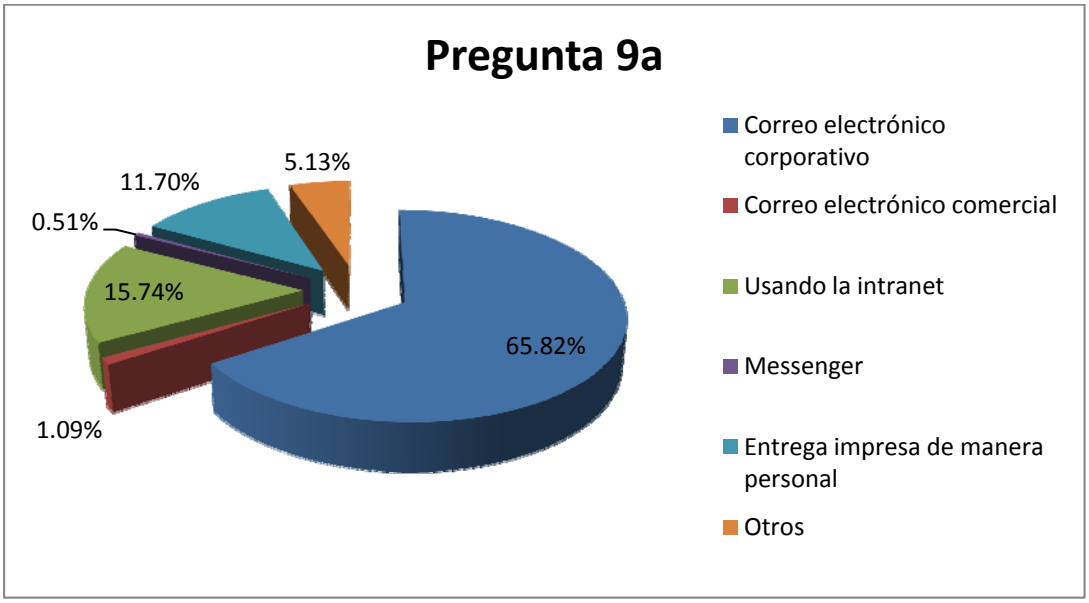
Finalmente, en cuanto a la conversación de temas laborales con amigos o compañeros que laboran en otras empresas del mismo giro, puede ser crucial ya que dependiendo del tipo de información revelada se considerará el grado de riesgo que tenga la institución ante esta circunstancia, para evitar dicha fuga de información se recomienda hablar con el personal para que se concientice respecto a la importancia que se tiene al evitar expresar información sensible de la empresa incluso con amigos y compañeros de otras instituciones similares, ya que esto puede generar en el peor de los casos un tipo de espionaje industrial que repercutiría en gran manera en el desarrollo y éxito de la institución.

Para la siguiente pregunta responda cada uno de los incisos

9. Por qué medio(s) transmite regularmente a sus jefes, compañeros o personal a su cargo:

a) La información de nuevos servicios de la empresa *

- [ ] Correo electrónico corporativo
- [ ] Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- [ ] Usando la intranet
- [ ] Messenger
- [ ] Entrega impresa de manera personal
- [ ] Other:

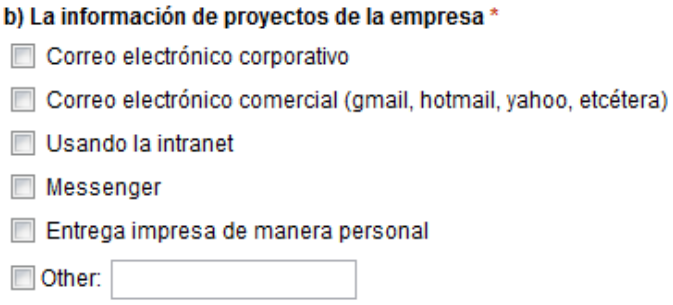


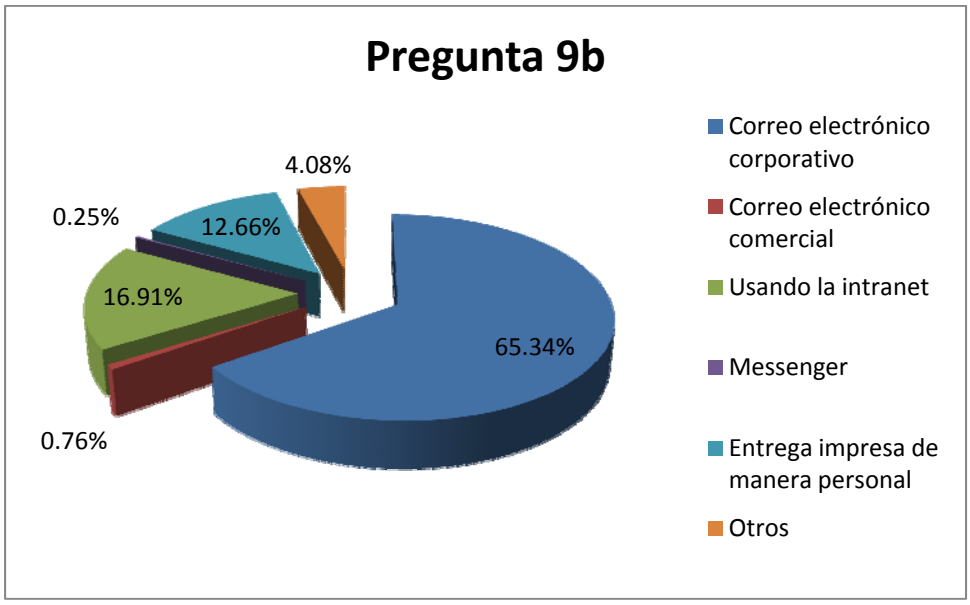
Interpretación: La pregunta número 9a se planteó con la finalidad de detectar los medios principales de comunicación que utilizan los empleados al momento de transmitir información relacionada con nuevos servicios de la empresa. Cabe señalar que para esta pregunta los empleados tuvieron la opción de elegir más de una respuesta. Los datos arrojados fueron los siguientes:

El 65.82% de los encuestados respondió que para transmitir entre sus compañeros información relacionada con nuevos servicios de la empresa lo hace a través del correo electrónico corporativo, hecho que refleja un cúmulo de buenas prácticas aplicadas por parte de los empleados y que seguramente el sector financiero difunde a todos los niveles jerárquicos. El segundo lugar lo obtiene, con un 15.74%, el envío de dicha información a través del uso de la intranet; mientras que el tercer lugar lo ha ganado, con un 11.70%, el uso de la entrega impresa de manera personal. Por otro lado, el 5.13% aseguró que emplea otros medios para transmitir dicha información, medios de comunicación tales como: el uso de la expresión oral de manera personal con los empleados interesados, lo tratan en juntas o reuniones laborales, utilizan audios, emplean el uso del teléfono, el uso de un servidor de contenidos, utilizan el correo electrónico comercial principalmente gmail, o bien dicha información no aplica a sus funciones laborales dentro de la institución. De esta última parte podemos observar que en su mayoría ese 5.13% representa el uso de la vía telefónica y la expresión oral en juntas convocadas para tratar dicha información con las partes interesadas, cuestión que habla muy bien de la técnica que utilizan los empleados para transmitir este tipo de información; sólo cabría la posibilidad de difundir a los trabajadores que sean cuidadosos al momento de transmitir dicha información por medio telefónico, ya que un tercer ente podría estar escuchando dicha información y emplearla con fines maliciosos.

Finalmente, se destaca que el 1.09% de los encuestados señaló que utiliza el corre o electrónico comercial, hecho que puede ser contraproducente debido a que la información que se envía a través de dicha vía es almacenada en las bases de datos de las empresas que proveen el servicio correspondiente y esto puede generar una fuga de información sensible que únicamente le compete su conocimiento a la institución.

Asimismo, se reflejó un 0.51% de los empleados que acostumbran a trasmitir dicha información a través del Messenger, este factor no se puede considerarse como grave a menos que la información que viaja a través de la red, por parte de los interesados, se haga de manera no cifrada, siendo así, si representaría un punto vulnerable para las instituciones financieras debido a que terceras personas podrían obtener la información transmitida que viaja a través de la red y utilizarla con otros fines.





Interpretación: La pregunta número 9b se planteó con la finalidad de detectar los medios principales de comunicación que utilizan los empleados al momento transmitir información referente a proyectos de la empresa. Cabe señalar que para esta pregunta los empleados tuvieron la opción de elegir más de una respuesta. Los datos arrojados fueron los siguientes:

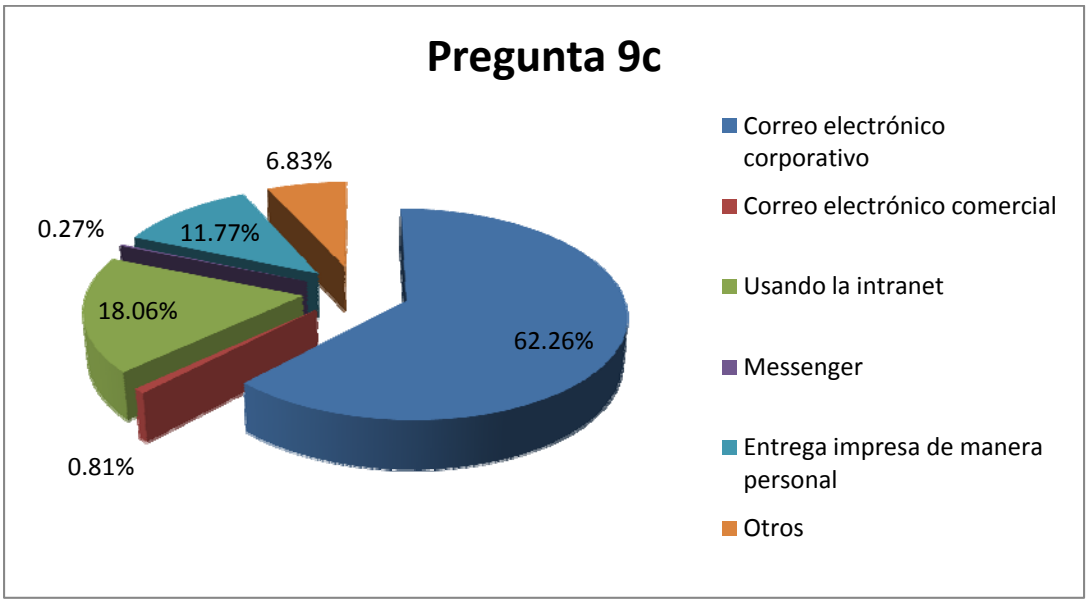
Se observa que un 65.34% de los empleados encuestados respondió que realiza dichas entregas a través del correo electrónico corporativo, el 16.91% aseguró hacerlo a través del uso de la intranet, mientras que el 12.66% efectúa dichas entregas de manera impresa y personalmente. Como se puede visualizar sigue extiendo la aplicación de buenas prácticas por parte de los empleados al transmitir información sensitiva.

Por otra lado un 4.08% de los empleados respondieron que utilizan otros medios de comunicación para transmitir información relacionada con proyectos de la empresa, tales como: presentaciones, reuniones o juntas en las que se expone dicha información de manera verbal, lo hacen personalmente de forma oral únicamente hacia las personas implicadas, toman en consideración las instrucciones de la institución, pasan la información a través de dispositivos de almacenamiento como USB, hacen uso de SICOP (Sistema de Contabilidad y Presupuesto), proporcionan la información dependiendo del tipo de proyecto del que se trate, o bien sus funciones no corresponden a tener acceso a dicha información, por lo tanto dicha pregunta no aplicó a una parte considerable de este porcentaje.

Asimismo, cabe resaltar que el restante 1.01% señaló que transmite dicha información a través del correo electrónico comercial y por medio del Messenger. Esta situación marca una similitud de respuesta a la pregunta anterior en donde el promedio del porcentaje de las personas que afirmaron utilizar el Messenger y el correo electrónico comercial para el envío de información fue del 1.6%, lo cual se ve reflejado con una diferencia del 0.59% en donde resalta el envío de información respecto a nuevos servicios de la empresa a través de estos medios.

c) La información de estudios de mercado de la empresa *

- [ ] Correo electrónico corporativo
- [ ] Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- [ ] Usando la intranet
- [ ] Messenger
- [ ] Entrega impresa de manera personal
- [ ] Other:



Interpretación: La pregunta número 9c se planteó con la finalidad de detectar los medios principales de comunicación que utilizan los empleados al momento transmitir información referente a estudios de mercado utilizados por la empresa. Cabe señalar que para esta pregunta los empleados tuvieron la opción de elegir más de una respuesta. Los datos arrojados fueron los siguientes:

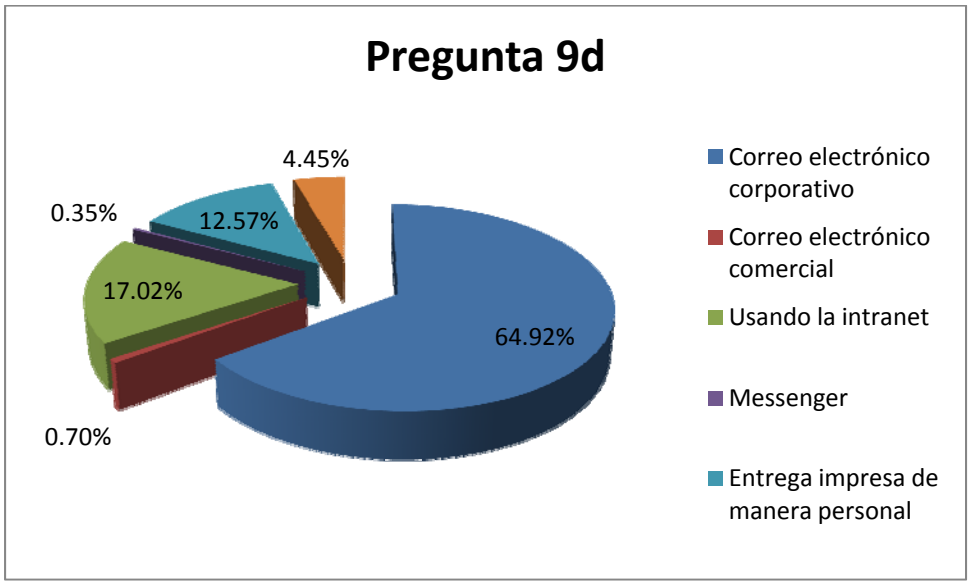
Con un porcentaje del 62.26% los empleados respondieron hacer uso de correo electrónico corporativo, el 18.06% afirmó que utiliza la intranet para ello, mientras que el 11.77% señala que utiliza la entrega impresa de manera personal. Dichos datos se ven ampliamente reflejados con las buenas prácticas aplicadas en las instituciones financieras, sobre todo para información de ésta índole.

Por otra parte, se puede visualizar, con un 6.83%, el uso de otros medios de comunicación para la transmisión de información referente a estudios de mercado, dichos medios señalados por los empleados tienen gran similitud a los mencionados en las preguntas anteriores tales como: la expresión oral de manera personal, el uso de presentaciones, la convocación a juntas y reuniones laborales, algunos otros admitieron que sólo transmiten dicha información si existe una autorización previa o bien sólo proporcionan algunos datos de interés y no toda la información, otros hacen uso del teléfono, mientras que una población considerable admitió que esa actividad no aplica a sus funciones o bien la desconocen.

Finalmente, el 1.08% restante, señaló que comparte dicha información a través de medios tales como el correo electrónico comercial o bien a través del Messenger (0.81% y 0.27% respectivamente). Cabe señalar que como se hizo mención en las preguntas anteriores el uso del Messenger no es malo, sin embargo, se recomienda la utilización de aplicaciones que cifren la información; y por otro lado, en lo referente al correo electrónico se recomienda hacer uso del correo electrónico institucional para el paso de información de estudios de mercado debido a que al hacer uso del correo electrónico comercial, dicha información tiende a quedar expuesta a terceras partes.

d) La información de reportes de actividades de la empresa *

- ☐ Correo electrónico corporativo
- ☐ Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- ☐ Usando la intranet
- ☐ Messenger
- ☐ Entrega impresa de manera personal
- ☐ Other:



Interpretación: La pregunta número 9d se planteó con la finalidad de detectar los medios principales de comunicación que utilizan los empleados al momento transmitir información con respecto a reportes de actividades derivados de las funciones realizadas dentro de la institución. Cabe señalar que para esta pregunta los empleados tuvieron la opción de elegir más de una respuesta. Los datos arrojados fueron los siguientes.

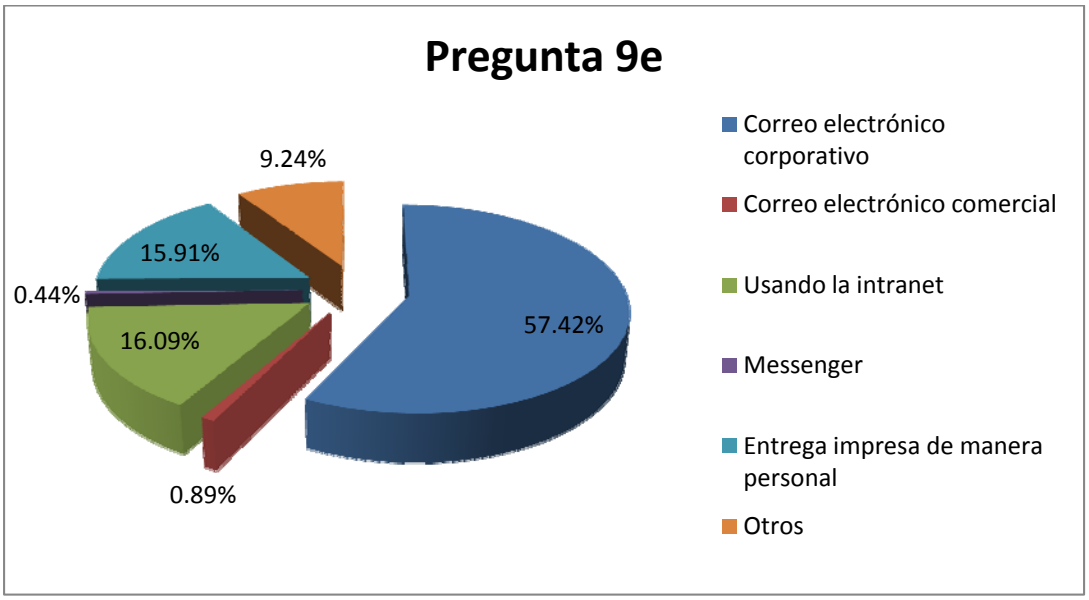
En el gráfico se puede observar que un 64.92% de los encuestados respondió que para transmitir este tipo de información lo hacen a través del correo electrónico corporativo, en segundo lugar, con un 17.02% de los empleados señaló que hace uso de la intranet; y en tercer lugar, se posiciona el uso de la entrega impresa de la información de manera personal con un 12.57%. Igualmente que en los casos anteriores se observa la aplicación de buenas prácticas por parte de los empleados.

Por otra parte, el 4.45% respondió que emplea el uso de otros medios de comunicación para transmitir información referente a reportes de actividades, de dichos medios resaltan el uso de presentaciones, la comunicación verbal de manera personal, el uso del teléfono, la utilización de un sistema especial de la institución, otros afirmaron utiliza gwa.b en línea o bien Microsoft Office Communicator, así mismo, reflejan hacer uso de dispositivos de almacenamiento tal como la USB; mientras que otra parte considerable respondió que dichos reportes no competen a sus actividades diarias.

Finalmente, el restante 1.05% respondió que comparte la información respecto a reportes de actividades a través de medios tales como el correo electrónico comercial o bien a través del Messenger (0.70% y 0.35% respectivamente). Cabe señalar que como se hizo mención en las preguntas anteriores el uso del Messenger no es malo; sin embargo, se recomienda la utilización de aplicaciones que cifren la información; y por otro lado, en lo referente al correo electrónico se recomienda hacer uso del correo electrónico institucional para la transferencia de información respecto a reportes de actividades por parte de los empleados debido a que al hacer uso del correo electrónico comercial dicha información tiende a quedar expuesta a terceras partes.

e) La información de nuevos productos antes de que salgan al mercado *

- ☐ Correo electrónico corporativo
- ☐ Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- ☐ Usando la intranet
- ☐ Messenger
- ☐ Entrega impresa de manera personal
- ☐ Other:



Interpretación: La pregunta número 9e se planteó con la finalidad de detectar los medios principales de comunicación que utilizan los empleados al momento transmitir información referente a productos de la institución antes de que salgan al mercado. Cabe señalar que para esta pregunta los empleados tuvieron la opción de elegir más de una respuesta. Los datos arrojados fueron los siguientes:

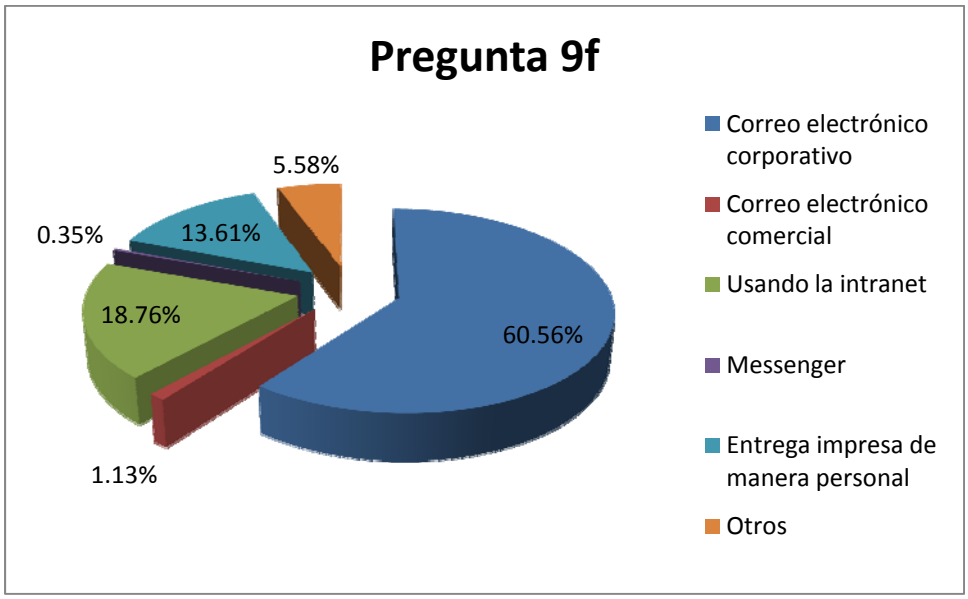
Se observa que un 57.42% de la población utiliza el correo electrónico corporativo como medio de transmisión principal de la información anteriormente expuesta; el segundo lugar lo ocupa, con un 16.09% de los encuestados, el uso de la intranet; y en tercer lugar se ubica la respuesta del uso de la entrega impresa de manera personal con un 15.91%. De estos datos se puede inferir que los empleados continúan haciendo buen uso de las buenas prácticas que probablemente las instituciones del sector financiero han establecido en sus políticas.

Por otra parte, se visualiza un 9.24% de los encuestados que respondieron hacer uso de otros medios de comunicación tales como la expresión verbal y de manera personal con los interesados, convocación de juntas o reuniones para discutir dichos asuntos, o bien la transmisión de circulares, otros tantos señalaron que no difunden la información antes de que salga al público y parte del porcentaje considerable señaló que dicha información no aplica a sus funciones, es decir, no poseen dicha información y por lo tanto no fungen como intermediaros para la difusión de la misma o bien la desconocen.

Finalmente, el 1.33% restante respondió que comparte la información respecto a nuevos productos de la institución antes de que salgan al público, a través de medios tales como el correo electrónico comercial o bien a través del Messenger (0.89% y 0.44% respectivamente). Cabe señalar que como se hizo mención en las preguntas anteriores el uso del Messenger no es malo; sin embargo se recomienda la utilización de aplicaciones que cifren la información; y por otro lado, en lo referente al correo electrónico se recomienda hacer uso del correo electrónico institucional para el paso de información de nuevos productos antes de que salgan a la luz, debido a que al hacer uso del correo electrónico comercial dicha información tiende a quedar expuesta a terceras partes y podría implicar un robo de ideas que repercutiría en la organización.

f) La información de servicios financieros *

- [ ] Correo electrónico corporativo
- [ ] Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- [ ] Usando la intranet
- [ ] Messenger
- [ ] Entrega impresa de manera personal
- [ ] Other:



Interpretación: La pregunta número 9f se planteó con la finalidad de detectar los medios principales de comunicación que utilizan los empleados al momento transmitir información referente a servicios financieros. Cabe señalar que para esta pregunta los empleados tuvieron la opción de elegir más de una respuesta. Los datos arrojados fueron los siguientes:

Como se puede observar en el gráfico, el 60.56% de los encuestados respondió que utiliza en primer lugar el correo electrónico corporativos para transmitir información referente a servicios financieros; en segundo lugar aparece, con un 18.76% el uso de la intranet; y en tercer lugar se coloca el uso de la entrega impresa de manera personal con un 13.61%. Al igual que en los datos estadísticos reflejados en las preguntas anteriores y afines a este rubro, se puede deducir que existe un uso continuo de buenas prácticas, por parte de los empleados, dentro de las instituciones que conforman el sector financiero.

Por otra parte, en lo que respecta a la respuesta de "otros", cabe señalar que ésta se vio reflejada con una incidencia del 5.58% de los empleados, los cuales indicaron que utilizan otros medios de comunicación tales como: presentaciones, comunicación oral y de manera personal únicamente al personal del área correspondiente, emiten dicha información según instrucciones por parte de la dirección responsable, otro conjunto aludió al uso de dispositivos de almacenamiento tal como la USB o bases de datos, utilización de la Herramienta de Colaboración de Google (*Google Docs*), la difusión hacia cualquiera que sea destacando que lo que interesa es que se conozca y difunda lo más pronto posible y al mayor número de gente que se pueda o bien su actividad no aplica la difusión de dicha información.

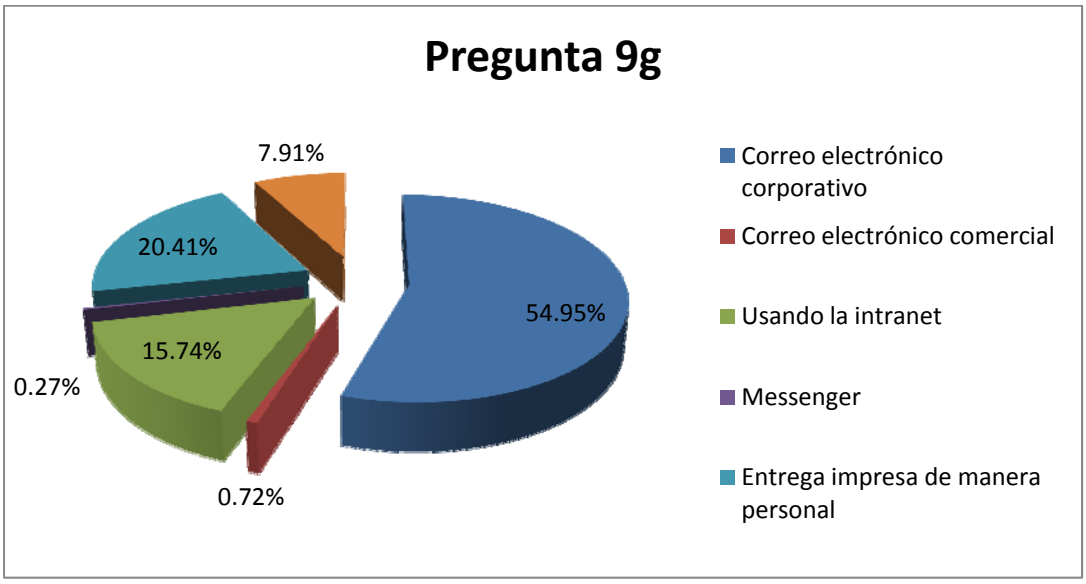
De estos datos cabe señalar que uso de herramientas colaborativas comerciales pueden ser de gran ayuda; sin embargo, la información queda expuesta en otros servidores, por lo que es recomendable hacer uso de aplicaciones colaborativas internas, tal como *Sharepoint, Visual Source Safe*, entre otras.

Finalmente, el restante 1.48% afirmó que comparte la información respecto a servicios financieros que brinda la institución, a través de medios tales como el correo electrónico comercial o bien a través del Messenger (1.13% y 0.35% respectivamente). Cabe señalar que como se hizo mención en las preguntas anteriores, el uso del Messenger no es malo; sin embargo, se recomienda la utilización de aplicaciones que cifren la información; y por otro lado, en lo referente al correo electrónico se recomienda hacer uso del

correo electrónico institucional para realizar la transferencia de información de los servicios financieros, debido a que al hacer uso del correo electrónico comercial dicha información tiende a quedar expuesta a terceras partes y podría implicar un robo de ideas que repercutiría en la organización. Sin embargo, cabe destacar, que los servicios financieros con los que cuentan las instituciones financieras son y se pretende que en su mayoría sean del conocimiento del público, por lo que este porcentaje sería despreciable para considerar que implique un riesgo para la organización.

g) Información respecto a contratos *

- [ ] Correo electrónico corporativo
- [ ] Correo electrónico comercial (gmail, hotmail, yahoo, etcétera)
- [ ] Usando la intranet
- [ ] Messenger
- [ ] Entrega impresa de manera personal
- [ ] Other:



Interpretación: La pregunta número 9g se planteó con la finalidad de detectar los medios principales de comunicación que utilizan los empleados al momento de transmitir información respecto a contratos. Cabe señalar que para esta pregunta los empleados tuvieron la opción de elegir más de una respuesta. Los datos arrojados fueron los siguientes:

Como se puede visualizar, el 54.95% de los empleados respondió que difunde éste tipo de información a través del uso del correo electrónico corporativo; el segundo lugar lo sostiene el 20.41% que corresponde a los empleados que señalaron hacer uso de la entrega impresa de manera personal; mientras que el tercer

lugar lo ocupa, con un 15.74%, el uso de la intranet. Al igual que en los datos estadísticos reflejados en las preguntas anteriores, y afines a este rubro, se puede deducir que existe un uso continuo de buenas prácticas, por parte de los empleados, dentro de las instituciones del sector financiero. Sin embargo, cabe destacar que existe una diferencia remarcada en cuanto a las respuestas de los incisos anteriores pertenecientes a la pregunta 9, como se puede observar existe un patrón repetible en los incisos a, b, c, d, e y f en los que se muestran que los primeros tres lugares de respuestas proporcionadas por los encuestados los ocupan el uso de correo electrónico corporativo, uso de intranet y la entrega impresa de manera personal respectivamente.

Por otro lado, un 7.91% de los encuestados señaló que hace uso de "otros" medios de comunicación para transmitir la información referente a contratos. De tales medios de comunicación resaltan: la entrega personal de manera verbal, la convocación de juntas o reuniones para brindar dicha información, el uso del teléfono, otros señalaron no utilizar ningún medio o bien respondieron que brindan dichos informes dependiendo de qué tipo de información de los contratos se requiera, otros empleados respondieron que no difunden este tipo de información, algunos tantos afirmaron hacerlo por medio de herramientas proporcionadas por la empresa, por medio de dispositivos de almacenamiento tal como USB o bien por medio de Bases de Datos ; así mismo, parte de los encuestados también respondió que dicha información no aplica a su área de trabajo. Dichos datos no reflejan un punto vulnerable; sin embargo, como recomendación respeto al uso de dispositivos de almacenamiento se recomienda que la información que en ellos se contenga sea almacenada de manera cifrada.

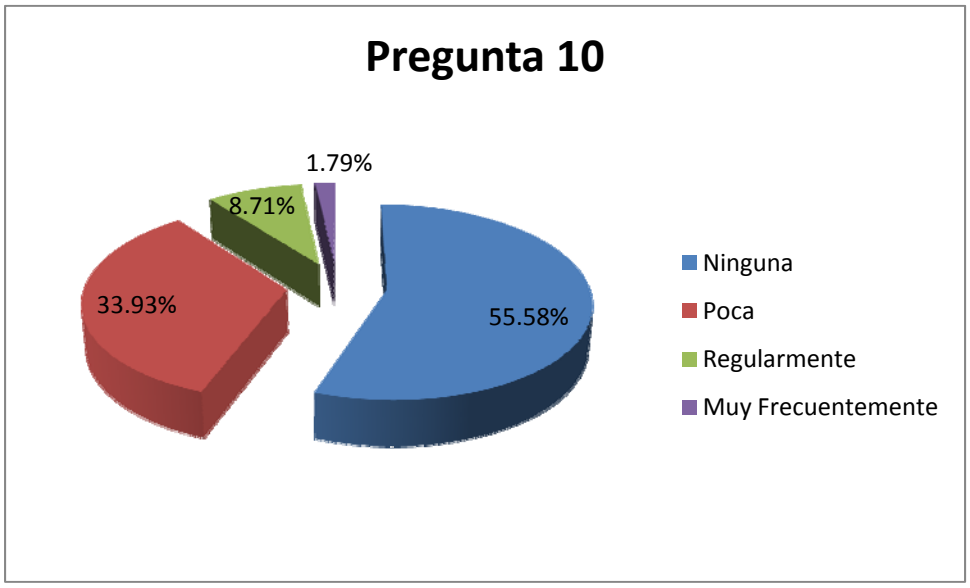
Finalmente, el restante 0.99% afirmó que comparte la información respecto a contratos, a través de medios tales como el correo electrónico comercial o bien a través del Messenger (0.72% y 0.27% respectivamente). Cabe señalar que como se hizo mención en las preguntas anteriores, el uso del Messenger no es malo; sin embargo, es recomendable la utilización de aplicaciones que cifren la información; y por otro lado, en lo referente al correo electrónico se recomienda hacer uso del correo electrónico institucional para la difusión de información respecto a los contratos, debido a que al hacer uso del correo electrónico comercial dicha información tiende a quedar expuesta a terceras partes y podría ser utilizada con fines maliciosos como la suplantación de identidad de los empleados, lo que implicaría un riesgo para la institución en el cual ésta sería susceptible de una mayor fuga de información sensitiva.

Para las siguientes preguntas, sólo se habilitó a los empleados la elección de una sola respuesta.

Par las siguientes preguntas seleccione sólo una opción

10. ¿Con qué frecuencia ha escuchado el término de la Ingeniería Social? *

Nada
Nada
Poco
Mucho
Muchísimo



Interpretación: En un intento por conocer si los empleados tienen noción del término de la Ingeniería Social, se planteó dicha pregunta, de la cual se obtuvieron los siguientes resultados:

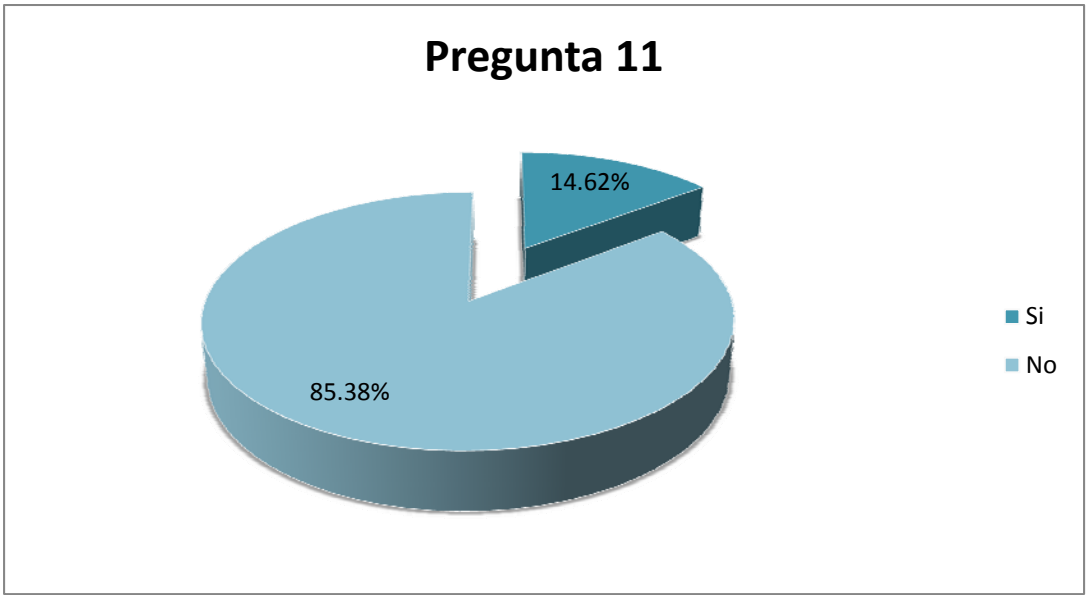
El primer lugar de las respuestas por parte de los empleados lo ocupa, con un 55.58%, el desconocimiento total del término "ingeniería social". Este resultado es grave y alarmante debido a que además de representar aproximadamente un sesenta por ciento de los encuestados, es importante resaltar que a falta del conocimiento de dicha técnica, que forma parte del hacking ético, se es mayoritariamente susceptible para divulgar información personal y confidencial de manera inconsciente, lo que podría poner en riesgo a las instituciones financieras debido a que agentes externos tendrían mayor oportunidad de obtener información sensible que podría ser utilizada con otros fines o bien en perjuicio de las organizaciones.

En segundo lugar, resalta con un 33.93% la respuesta de poco conocimiento respecto a la ingeniería social por parte de los empleados; mientras que el tercer lugar lo ocupan aquellos empleados que afirmaron saber mucho respecto al tema con un 8.71%, dicho porcentaje podría reflejarse únicamente en las personas que cuentan con carreras afines a las Ingenierías en Computación, Sistemas e Informática. Asimismo, con un 1.79% de los empleados encuestados, se destaca la respuesta que se tiene un conocimiento amplio respecto al tema en cuestión, porcentaje que refleja un bajo nivel de conocimiento por parte de los empleados respecto al tema. Para mermar este desconocimiento se recomienda difundir el tema ampliamente a todas las áreas de las organizaciones que forman parte del sector financiero y con ello las instituciones se asegurarán de que la divulgación de información sensible no sea difundida por los empleados a personas

externas a las organizaciones en las que laboran, ya que una vez que conozcan la técnica de la Ingeniería Social, tomarán las medidas pertinentes al momento de transmitir información referente a la institución.

11. ¿Utiliza la Ingeniería Social? *

- Si
- No



Interpretación: La pregunta número 11 se realizó con la finalidad de reafirmar la pregunta anterior, ya que en la mayoría de las ocasiones las personas se abstienen de responder que tienen una carencia del conocimiento respecto a un determinado tema, por lo que esta pregunta ayudó a confirmar si efectivamente el porcentaje señalado que indicó que "si conoce" el término de la ingeniería social, coincide con el porcentaje de expertos en el tema y de aquellos que tienen conocimiento respecto al mismo y por consiguiente saben en qué momento aplicar la técnica de la ingeniería social. El porcentaje total de los encuestados que afirmaron conocer el término de la ingeniería social en mayor escala, como se puede observar en la pregunta 10, representa el 10.5% (8.71% + 1.79%). De los datos obtenidos en esta pregunta se obtuvo lo siguiente:

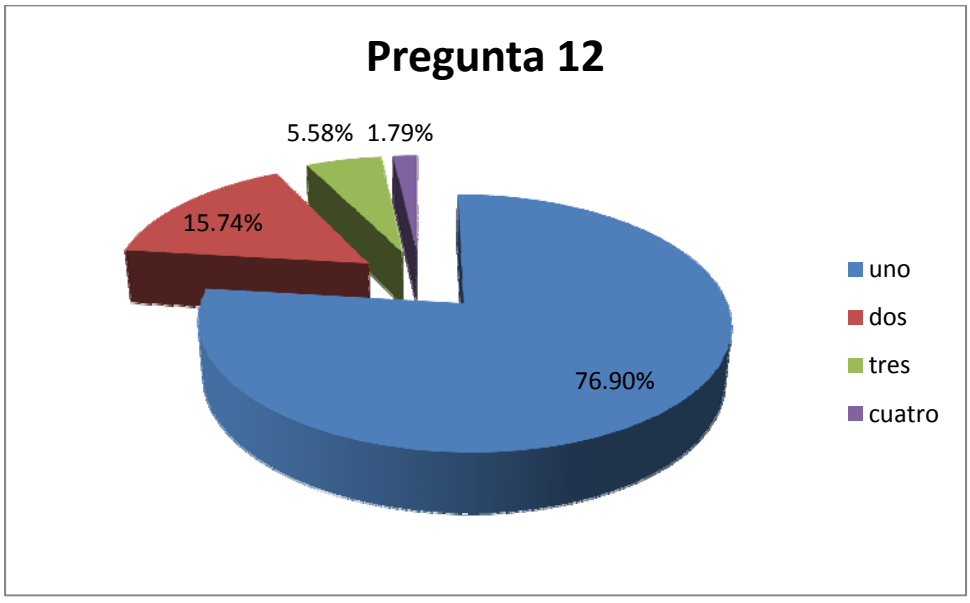
El 85.38% de los encuestados respondió que "no" hace uso de la ingeniería social, lo que podría interpretarse como falso ya que inconscientemente hacemos uso de dicha técnica, sólo que, la mayoría de las personas, debido al desconocimiento que tienen respecto a dicha técnica, no saben que al momento de entablar una conversación con sus semejantes podrían estar aplicando la ingeniería social sin saberlo o bien podrían ser víctimas de la misma. Sin embargo, con dicha estadística se comprueba una vez más que el desconocimiento que se tiene en el sector financiero respecto al tema es amplio.

Por otra parte, el 14.62% de los empleados restantes, respondió que sí hace uso de la ingeniería social, sin embargo, al comparar dicho porcentaje con el obtenido de la suma de aquellos empleados que

respondieron saber mucho respecto al tema y ser expertos del mismo, el cual representó un 10.5%, sobresale un 4.12% desfasado, de lo cual se puede interpretar que de los empleados que respondieron que "si" aplican dicha técnica, un poco más del 4% no quiso sentirse descartado del hecho de desconocer el tema, sin embargo, una vez más se reafirma la hipótesis respecto a que la mayoría de los empleados que trabajan en instituciones financieras no tienen conocimiento referente al tema de la ingeniería social y esto puede ser grave ya que propiciaría que los trabajadores puedan ser víctimas de un tercer ente que les aplique dicha técnica, logrando substraer información sensible, tanto personal como laboral del empleado, sin que ellos lo perciban.

12. En una escala del 1 al 4 ¿Con qué frecuencia se han experimentado ataques de tipo Pharming en su organización? *
El pharming es una modalidad de ataque informático, que consiste en suplantar al Sistema de Resolución de Nombres de Dominio (DNS, Domain Name System) con el propósito de conducirte a una página Web falsa.

	1	2	3	4	
Nunca	○	○	○	○	Muy frecuentemente



Interpretación: Dicha pregunta se efectuó con la finalidad de conocer si el personal que labora en la institución tiene conocimiento respecto a los ataques informáticos que comúnmente se suscitan en el sector financiero, en éste caso el ataque de tipo *Pharming*. De dicha pregunta se obtuvieron los siguientes resultados:

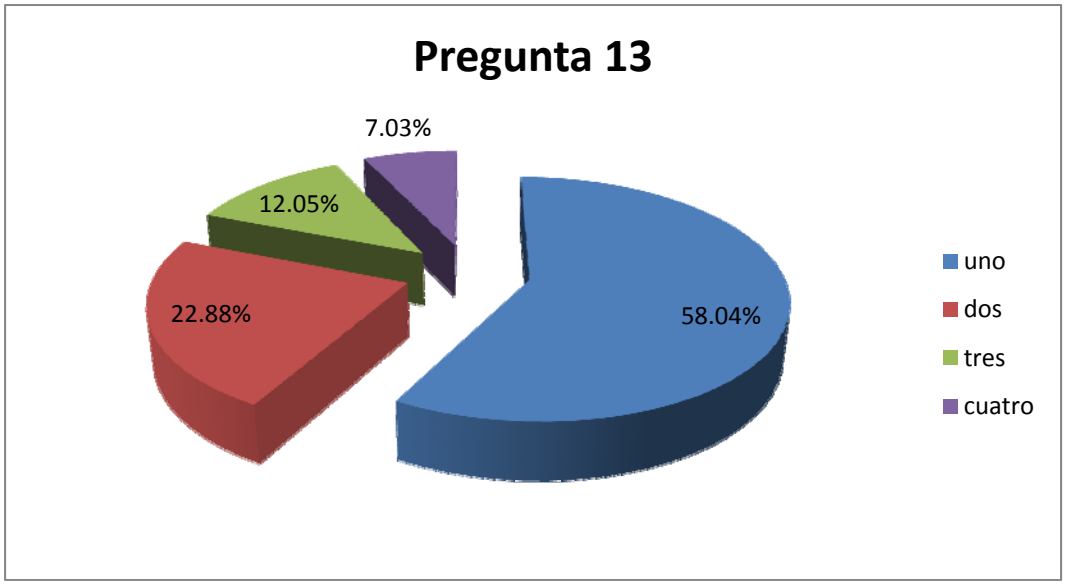
Con un 76.90% se refleja que los empleados encuestados respondieron que la institución nunca ha sido blanco de este tipo de ataque, sin embargo, cabe la posibilidad que dicha respuesta pueda representar desconocimiento del tema por parte de los empleados respecto al ataque informático de tipo *Pharming*,

hecho que es importante ya que como cultura general y al ser partícipes de una organización en donde existe la posibilidad de ser susceptible ante este tipo de ataque informático, es elemental, para que posteriormente los empleados tomen las medidas necesarias para evitar la propagación y ejecución del mismo.

Así mismo, se puede observar que un 15.74% de los encuestados respondió, que a su punto de vista, se han presentado muy pocos ataques informáticos de tipo *Pharming*; mientras que el 5.58% afirma que la presencia de dicho ataque se da con frecuencia en las instituciones financieras y el otro 1.79% respondió que tal ataque es muy frecuente en las organizaciones financieras. De dichos datos se puede concluir que es posible que gran parte de los empleados que respondieron a la escala de "dos", "tres" y "cuatro" tenga los conocimientos referente a este tipo de ataque informático y por ello aportan su estimación, sin embargo, cabe resaltar que existe un alto porcentaje de los encuestados que desconoce en qué consiste dicho ataque informático y eso es grave, debido a que al permitir que los empleados carezcan de capacitación y nociones respecto a éste tipo de ataque cuya presencia es común en el ámbito financiero, representa un punto vulnerable en las instituciones, hueco de seguridad del que algún atacante informático se podría aprovechar atentando contra la disponibilidad, confidencialidad e integridad de la información sensible con la que cuentan las instituciones.

13. En una escala del 1 al 4 ¿Qué tanto conocimiento tiene acerca del ataque de tipo Phising en su organización? *

	1	2	3	4	
Desconocimiento	◯	◯	◯	◯	Conocimiento



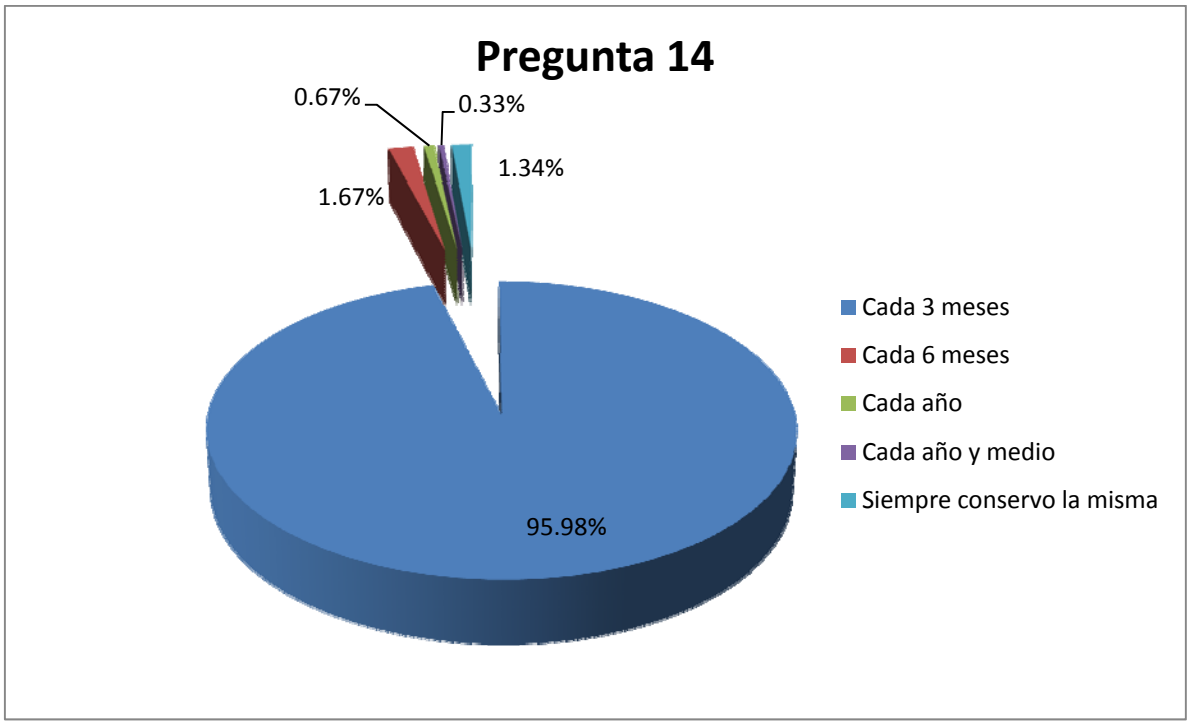
Interpretación: Dicha pregunta se efectuó con la finalidad de conocer si el personal que labora en la institución tiene conocimiento respecto a los ataques informáticos que comúnmente se suscitan en el sector financiero, en éste caso el ataque de tipo *Phising*. De dicha pregunta se obtuvieron los siguientes resultados:

Un 58.04% de los encuestados respondió que tiene un total desconocimiento respecto al tema, lo cual es muy preocupante ya que confirma lo expuesto en la pregunta anterior que alude a que los empleados tienen un amplio desconocimiento respecto a ataques de tipo informático presentados con frecuencia en el ámbito financiero. Por otra parte, en segundo lugar se posiciona la respuesta de los empleados que señalaron contar con "poco" de conocimiento respecto al tema y esto se ve reflejado con un 22.88%; subsecuentemente se puede apreciar que el 12.05% de los encuestados conoce lo referente a éste tipo de ataque informático, mientras que un 7.03% afirma que tiene un conocimiento experto del mismo.

De dichos resultados se puede destacar que un gran porcentaje de los empelados pertenecientes a las distintas áreas de las instituciones del sector financiero, desconocen en su totalidad los tipos de ataques informáticos más comunes que acontecen dentro y fuera del sector financiero, situación preocupante debido a que implicaría que los empleados podrían ser susceptibles a este tipo de ataque, dentro de las instituciones, sin saberlo; por ello se recomienda difundir platicas y conferencias respecto a los diferentes tipos de ataques informáticos, no sólo presentados dentro del ámbito financiero, sino también aquellos que se presentan con frecuencia de manera general al hacer uso de los equipos de trabajo. La finalidad de esta recomendación es que la empresa pueda mermar la exposición al riesgo al que se enfrenta y que los empleados puedan detectar eficazmente este tipo de irregularidades para que se mermen a la brevedad posible.

14. ¿Con qué frecuencia acostumbra a cambiar sus contraseñas? *

- ○ Cada 3 meses
- ○ Cada 6 meses
- ○ Cada año
- ○ Cada año y medio
- ○ Siempre conservo la misma



Interpretación: Dicha pregunta se efectuó con la finalidad de conocer si dentro de las políticas de las instituciones de banca múltiple y de banca de desarrollo se considera el cambio de la contraseña de los recursos utilizados por los empleados, tales como cuentas de correo, cuenta de intranet, contraseña del equipo asignado, etcétera. Así mismo, con esto se pretende conocer la cultura de seguridad de la información con la que cuentan los empleados ya que si este caso es afirmativo implicaría que los trabajadores realizan el cambio de las contraseñas de manera frecuente, de lo contrario existiría un peligro latente para las instituciones.

Del gráfico se puede visualizar que un 95.98% de los empleados encuestados tiene la buena práctica de cambiar sus contraseñas cada 3 meses, un 1.67% la cambia cada 6 meses, el 1.34% conserva siempre la misma contraseña, mientras que el 0.67% y el 0.33% lo hacen cada año y cada año y medio respectivamente.

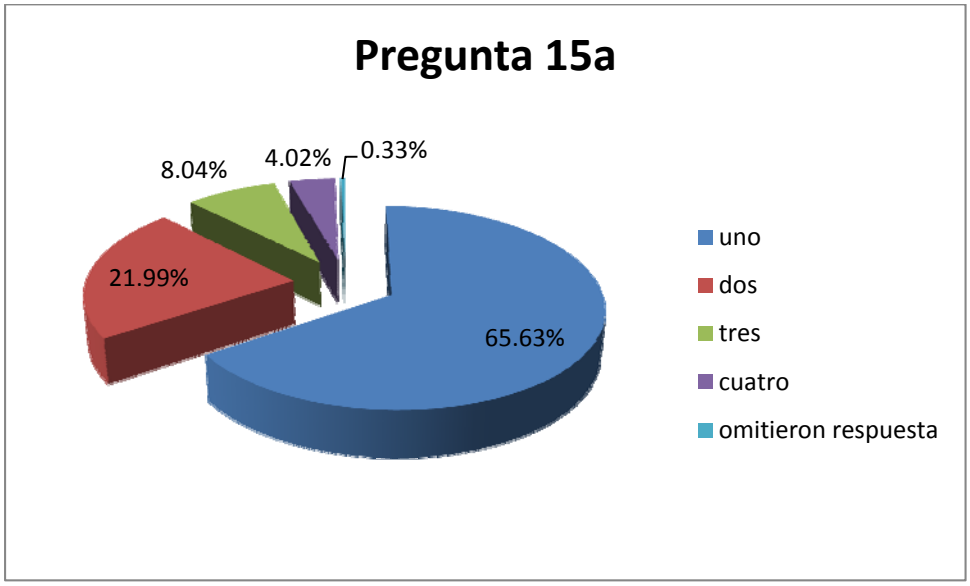
De tales datos se puede concluir que las instituciones, dentro del sector financiero, cuenta con políticas que señalan el cambio frecuente de las contraseñas, en su mayoría cada tres meses, sin embargo, es preocupante que el tercer lugar lo ocupa, con un 1.34% de los encuestados, la respuesta respecto a que los empleados siempre conservan la misma contraseña, factor que se hace sobresaliente, ya que el mantener la misma contraseña por tiempos prolongados, puede generar que los empleados sean blanco fácil de ataques informáticos externos e incluso internos realizados por terceras personas. Sin embargo, para dicho caso se resalta que aunado al cambio de contraseña también es importante difundir una cultura del uso de contraseñas robustas, las cuales deberán contener: letras mayúsculas y minúsculas, números, así como caracteres especiales, además de que la longitud de la misma se recomienda sea mayor a 8 caracteres.

En una escala del 1 al 4,

15. ¿Con qué frecuencia responde encuestas o cuestionarios que no sean corporativos:?

a) Dentro de la institución

	1	2	3	4	
Nunca	○	○	○	○	Muy frecuentemente



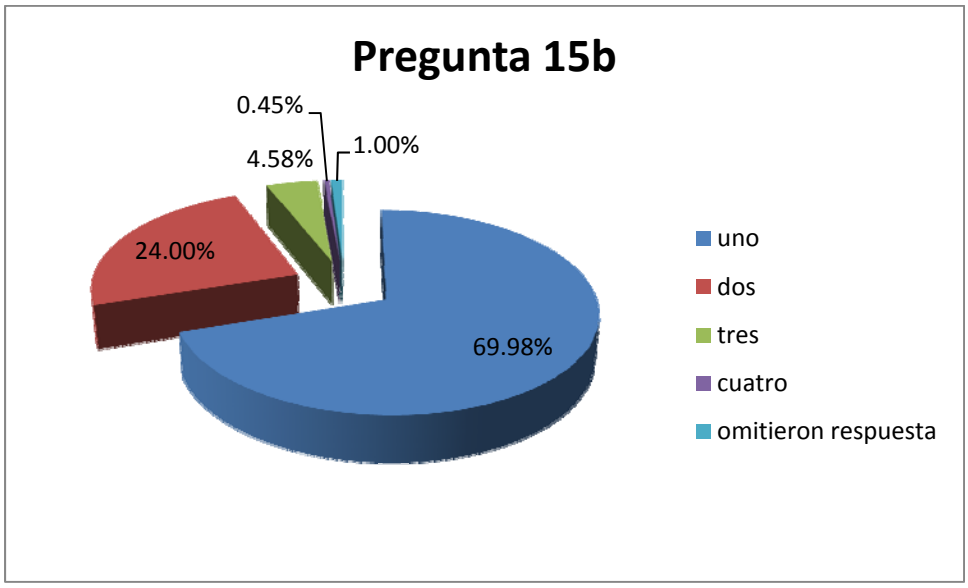
Interpretación: De dicha pregunta, cuyo objetivo fue conocer la frecuencia con la que participan los empleados en encuestas efectuadas dentro de las instituciones. Para lo cual se obtuvieron los siguientes resultados:

Un 65.63% de los encuestados afirma que nunca responde este tipo de encuestas; en segundo lugar con un 21.99% se colocan los empleados que acostumbran a responder pocas encuestas. El tercer lugar corresponde a aquellos encuestados que señalan responder frecuentemente este tipo de encuestas con un 8.04%, mientras que el 4.02% afirma que lo hace muy frecuentemente y el otro 0.33% restante omitió dar respuesta a la pregunta.

De tales datos se puede destacar que al suscitarse encuestas dentro de la institución referente a cuestiones no corporativas, no es común la participación de los empleados, de lo cual se puede resaltar que cuando las encuestas no son de índole institucional o bien obligatorias, los empleados se abstienen de contestar a las mismas debido a que cabe la posibilidad de que les resulte indiferente.

b) Fuera de la institución

	1	2	3	4	
Nunca	○	○	○	○	Muy frecuentemente



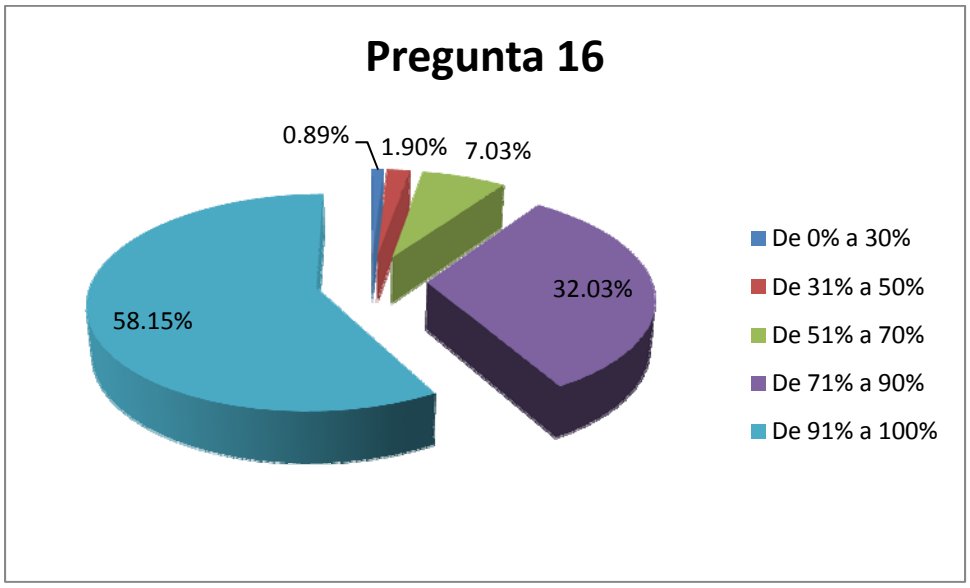
Interpretación: La pregunta número 15b se realizó con la finalidad de conocer si los empleados de la institución responden con frecuencia encuestas o cuestionarios fuera de la institución. Los resultados arrojados fueron los siguientes:

Se observa que un 69.98% de los encuestados afirma que nunca responde este tipo de encuestas; en segundo lugar con un 24% se colocan los empleados que acostumbran a responder pocas encuestas. El tercer lugar corresponde a aquellos encuestados que indicaron que responden frecuentemente este tipo de encuestas con un 4.58%, mientras que el 0.45% afirma que lo hace muy frecuentemente y el otro 1% restante omitió dar respuesta a la pregunta.

De tales datos se puede destacar que el hecho de contestar encuestas fuera de la institución referentes a cuestiones laborales, no implica un peligro directo para la organización, sin embargo, es importante recalcar a los empleados que el tipo de información que se plasme en dichas encuestas no debe ser de índole confidencial, debido a que al hacerlo pueden comprometer la seguridad de la información de la organización en la que laboran. Así mismo, como se puede visualizar, el porcentaje de los empleados encuestados que respondió que contribuye a encuestas fuera de la organización de manera frecuente, es mínimo, por lo que no implica riesgo alguno para las instituciones de banca múltiple y de banca de desarrollo, pero sí se recomienda tomar en consideración los puntos tratados con anterioridad en éste párrafo.

16. ¿Con qué porcentaje de seguridad de la información estima que cuenta su organización? *

De 0% a 30%	De 31% a 50%	De 51% a 70%	De 71% a 90%	De 91% a 100%
○	○	○	○	○



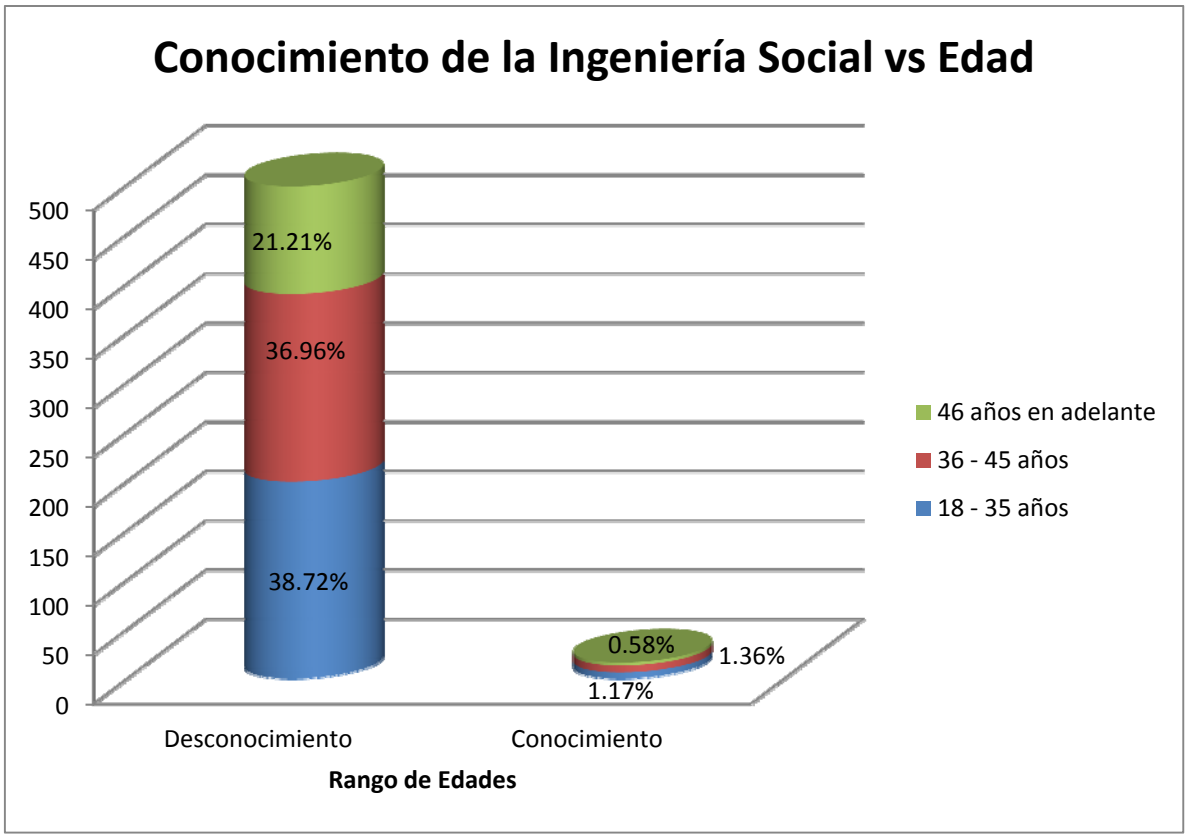
Interpretación: Esta pregunta fue elaborada con la intención de conocer la percepción que tienen los empleados de la institución respecto a la seguridad de la información de la misma. Los resultados obtenidos fueron los siguientes:

Con un 58.15% resalta la perspectiva de los empleados de que las instituciones en análisis cuentan con un porcentaje alto, con respecto a la seguridad de la información existente, dentro de la organización, éste porcentaje oscila entre el rango del "91% y el 100%". En segundo lugar se posiciona, con un 32.03% de respuestas afirmativas, el porcentaje de seguridad de la información estimado del "71% al 90%". Posteriormente, un 7.03% de los encuestados respondió que su institución cuenta con un nivel de seguridad de la información del "51% al 70%", mientras que el 1.90% de los empelados respondió que su perspectiva respecto a la seguridad de la información que maneja la organización es del "31% al 50%"; el otro 0.89% restante lo abarcan las perspectivas por parte de los empleados del "0% al 30%".

Finalmente, de los datos arrojados durante la encuesta, se puede concluir que la mayoría de los empleados tienen una perspectiva favorable de la institución con respecto al ámbito de la seguridad de la información, sin embargo, no se descarta la existencia de una perspectiva pequeña, por parte de los empleados, que alude a que la seguridad de la información existente en la organización es "baja". Sería interesante realizar un monitoreo por medio de encuestas para conocer los motivos que propician que los trabajadores expresen esto. Así mismo, este porcentaje podría reflejar una baja fidelidad ante las instituciones por parte de sus empleados, lo que podría generar conflictos que recaigan en fugas de información suscitadas de adentro hacia afuera de la institución, se recomienda estar al pendiente de dichos factores.

5.3 CORRELACIONES

A continuación se muestran correlaciones respecto a distintos rubros de datos combinados, que en su conjunto responden a las preguntas de investigación planteadas. Cabe resaltar que el eje de las ordenadas "y" no tiene significancia en el trazado de lso datos, únicamente se colocó para dar escala a las gráficas presentadas. A continuación se muestran los resultados:

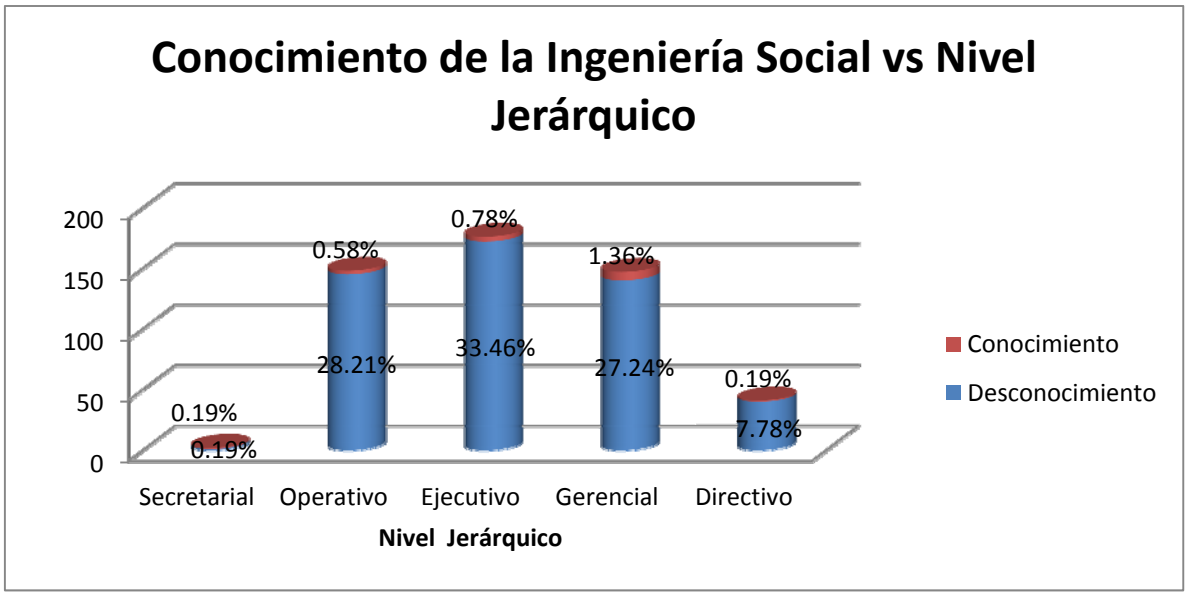


Interpretación: Con respecto a la correlación de los datos que se hizo referente al conocimiento o desconocimiento que los encuestados tienen respecto a la ingeniería social, se decidió correlacionar dicho dato con las edades de los mismos, con la finalidad de corroborar si la edad influye en cuanto al conocimiento que se debería tener respecto al tema de la ingeniería social.

Como se puede observar la gráfica se divide en dos vertientes, la primera de ellas muestra los porcentajes que los empleados encuestados reflejaron al indicar que no tienen conocimiento alguno sobre la Ingeniería Social, mientras que la segunda barra refleja el porcentaje de los empleados, por edades, que aseguró tener conocimiento respecto al tema. De dicha gráfica podemos deducir lo siguiente:

Existe un total del 96.98% de los encuestados que aseguró desconocer el tema de la Ingeniería Social, sin embargo, aludiendo al rango de las edades, el 38.72% corresponde a edades de los 18 a 35 años, el segundo lugar lo obtener el rango de edades de los 36 a 45 años de edad con un 36.96% ,y en tercer y último lugar, se posiciona con un 21.21% el rango de edades de los 46 años en adelante, que aseguraron desconocer totalmente el tema. Por otro lado, en la barra que refleja el porcentaje de empleados que aseguró conocer el tema en cuestión, se tiene que el rango de edades de los empleados que respondieron ser conocedores del tema de la ingeniería social comprende el rango de edades de los 36 a los 45 años de edad, mientras que en segundo lugar se posicionan con un 1.17% los encuestados del rango de edades de los 18 a los 35 años, y en tercer lugar se colocan con un 0.58% los empleados cuyas edades comprenden el rango de los 46 años en adelante.

De tales datos podemos inferir que respecto al tema de la Ingeniería Social, la edad no influye en que los empleados conozcan o desconozcan el tema, ya que como bien se podría haber previsto desde un principio al argumentar que existiera una mayor posibilidad de que los encuestados del rango de las edades de los 18 a los 35 años conocieran el tema debido a que son generaciones que se encuentran involucradas constantemente con la tecnología y la seguridad informática, los resultados han refutado totalmente dicho pensamiento, lo que permite concluir que en todos los rangos de edades posibles existe un desconocimiento total respecto al tema en cuestión y esto es grave debido a que se puede ser susceptible a la técnica de la Ingeniería Social que puede ser aplicada en el ámbito malicioso, lo que generaría grandes fugas de información confidencial y por consiguiente la confidencialidad de la información de las instituciones quedaría expuesta a terceros.



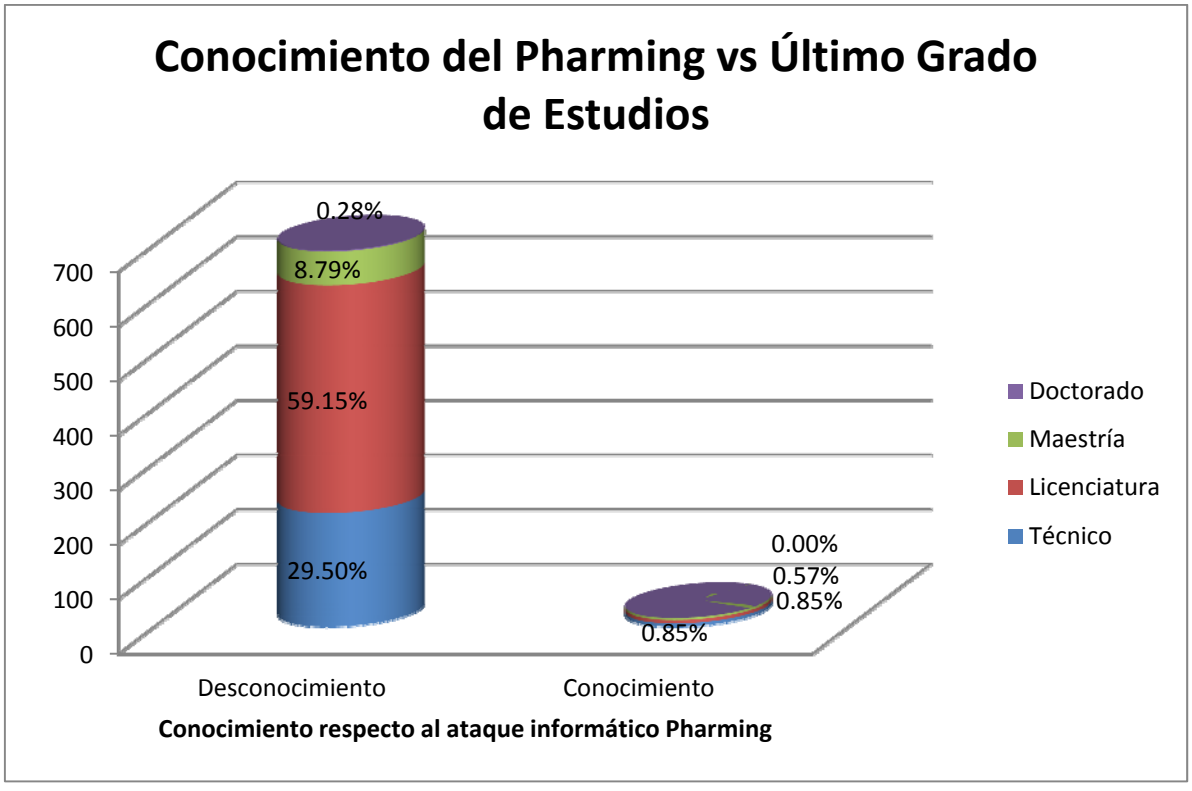
Interpretación: Con respecto a la correlación de los datos que se hizo referente al conocimiento o desconocimiento que los encuestados tienen respecto a la ingeniería social, se decidió correlacionar dicho dato con el nivel jerárquico de los mismos, con la finalidad de corroborar si el nivel jerárquico influye en cuanto al conocimiento que se debería tener respecto al tema de la ingeniería social.

Como se puede observar la gráfica se divide en dos vertientes, la primera de ellas muestra los porcentajes que los empleados encuestados reflejaron al indicar que no tienen conocimiento alguno sobre la Ingeniería Social, mientras que la segunda barra refleja el porcentaje de los empleados, por nivel jerárquico, que aseguró tener conocimiento respecto al tema. De dicha gráfica podemos deducir lo siguiente:

Como se puede visualizar en las cuatro gráficas, el color azul refleja un desconocimiento total respecto al tema de la ingeniería social, sin embargo es importante interpretar en qué nivel jerárquico se da un mayoritario conocimiento respecto a la Ingeniería Social, lo cual se refleja con el color rojo. De la gráfica se observa que a nivel Gerencial, con un 1.36%, existe un mayor porcentaje de los encuestados que afirmó que cuentan con un conocimiento sólido respecto al tema de la Ingeniería Social, es decir, saben qué es, en qué consiste y cómo se aplica; en segundo lugar se posiciona el nivel Ejecutivo con un 0.78% y el tercer lugar lo obtiene el nivel operativo con un 0.58%. Así mismo, se observa que el nivel jerárquico que tiene una menro

participación en cuanto al conocimiento del tema es el nivel Secretarial con un 0.19% al igual que el nivel Directivo que tiene una incidencia con el mismo porcentaje.

De lo anteriormente expuesto se puede concluir que de acuerdo al nivel jerárquico, si se tiene una inferencia en el conocimiento respecto a la Ingeniería social. Esto lo podemos observar al visualizar que el nivel "Gerencial" ocupa un porcentaje mayor de los encuestados que respondieron tener un sólido conocimiento respecto al tema de la Ingeniería Social, y mucho tiene que ver con el puesto ya que el nivel Gerencial es un filtro entre los niveles Directivos y Ejecutivos. Por otro lado, es preocupante que el nivel "Directivo" tenga una menor impacto en cuanto al conocimiento respecto a la Ingeniería Social al igual que el nivel "Secretarial", si analizamos esta información a detalle podremos darnos cuenta que los niveles secretariales trabajan conjuntamente con los niveles directivos y la carencia de éste conocimiento podría afectar gravemente la confidencialidad de la información divulgada, sin embargo, cabe señalar que los niveles directivos suelen transferir cada uno de los asunto suscitados en su campo laborar, a sus subordinados y especialistas en la materia, lo cual también se vio reflejado al momento de intentar aplicar el instrumento en las instituciones correspondientes, y fue precisamente en éstos rangos (Gerenciales, Ejecutivos y Operativo) en dónde se encontraron obstáculos para continuar con la investigación.



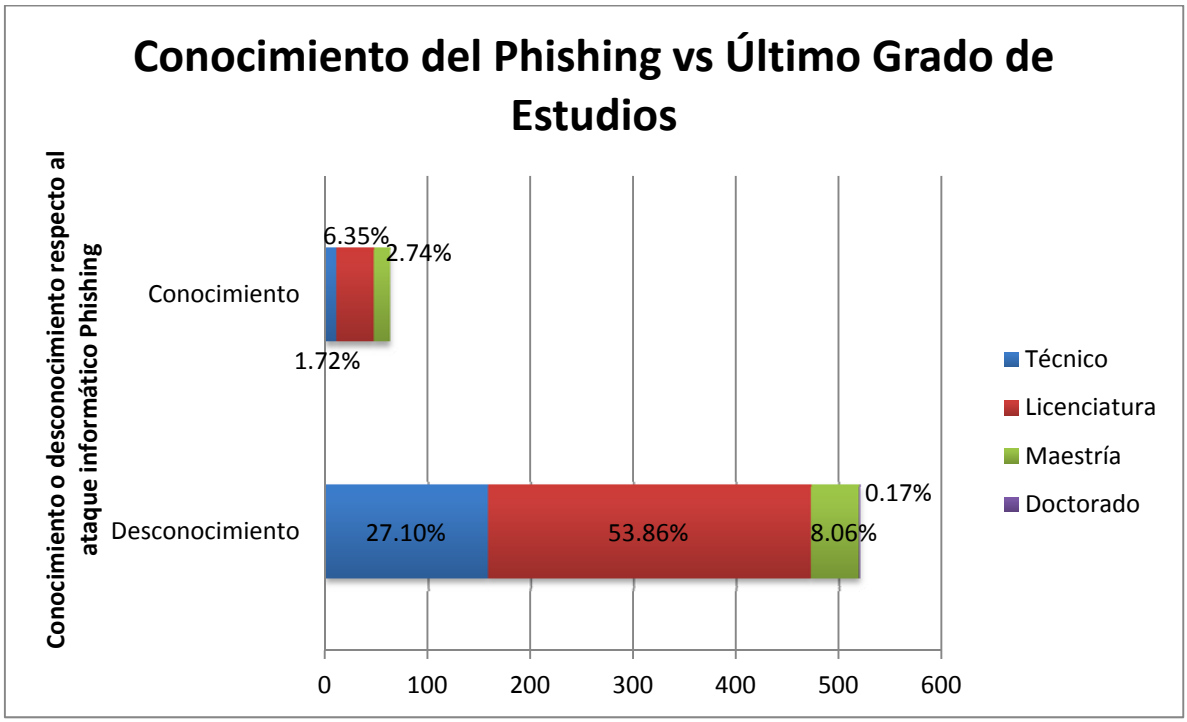
Interpretación: Con respecto de la correlación de los datos que se hizo referente al conocimiento o desconocimiento que los encuestados tienen respecto a uno de los ataques informáticos presentados con mayor frecuencia en el ámbito financiero "Pharming", se decidió correlacionar dicho dato con el último grado de estudios con el que cuentan los empleados encuestados, esto con la finalidad de corroborar si el

Grado de Estudios de los empleados encuestados tiene influencia en el conocimiento que se tiene de los ataques informáticos a los que están expuestos al hacer uso de un equipo de cómputo y/o comunicaciones.

De los datos arrojados en el gráfico se puede destacar que a nivel licenciatura existe un mayor desconocimiento respecto al ataque informático de tipo Pharming debido a que representa el 59.15%, mientras que el nivel doctoral se ve reflejado con un 0.28% que representa la menor parte proporcional.

Por otro lado, en la barra que lleva por nombre "Conocimiento" se reflejan las respuestas de los empleados que aseguraron conocer totalmente el tema, de la cual podemos extraer que, en primer lugar se posicionan con un 0.85% los empleados cuyo nivel de estudios es el de Licenciatura al igual que el nivel Técnico y en segundo lugar con un 0.57% se sitúan aquellos empleados que cuentan con una Maestría.

De esto se puede concluir que si existe una correlación activa entre el último grado de estudios y el conocimiento que se tiene respecto al ataque informático de tipo Pharming; sin embargo, ésta es débil, debido a que los porcentajes también se ven afectados con el número de empleados que labora en la institución y que según los datos arrojados en el capítulo anterior reflejaron un mayor índice de empleados cuyo grado de estudios representativo fue el nivel Licenciatura y nivel Técnico. Asimismo, es importante resaltar la preocupación que existe al observar que un porcentaje mayor se vea reflejado en respuestas de un "total desconocimiento" por parte de los empelados respecto al tema, lo que podría propiciar que los trabajadores sean un blanco fácil ante ataques informáticos presentados, no sólo de éste tipo, sino de índole informático de manera general.



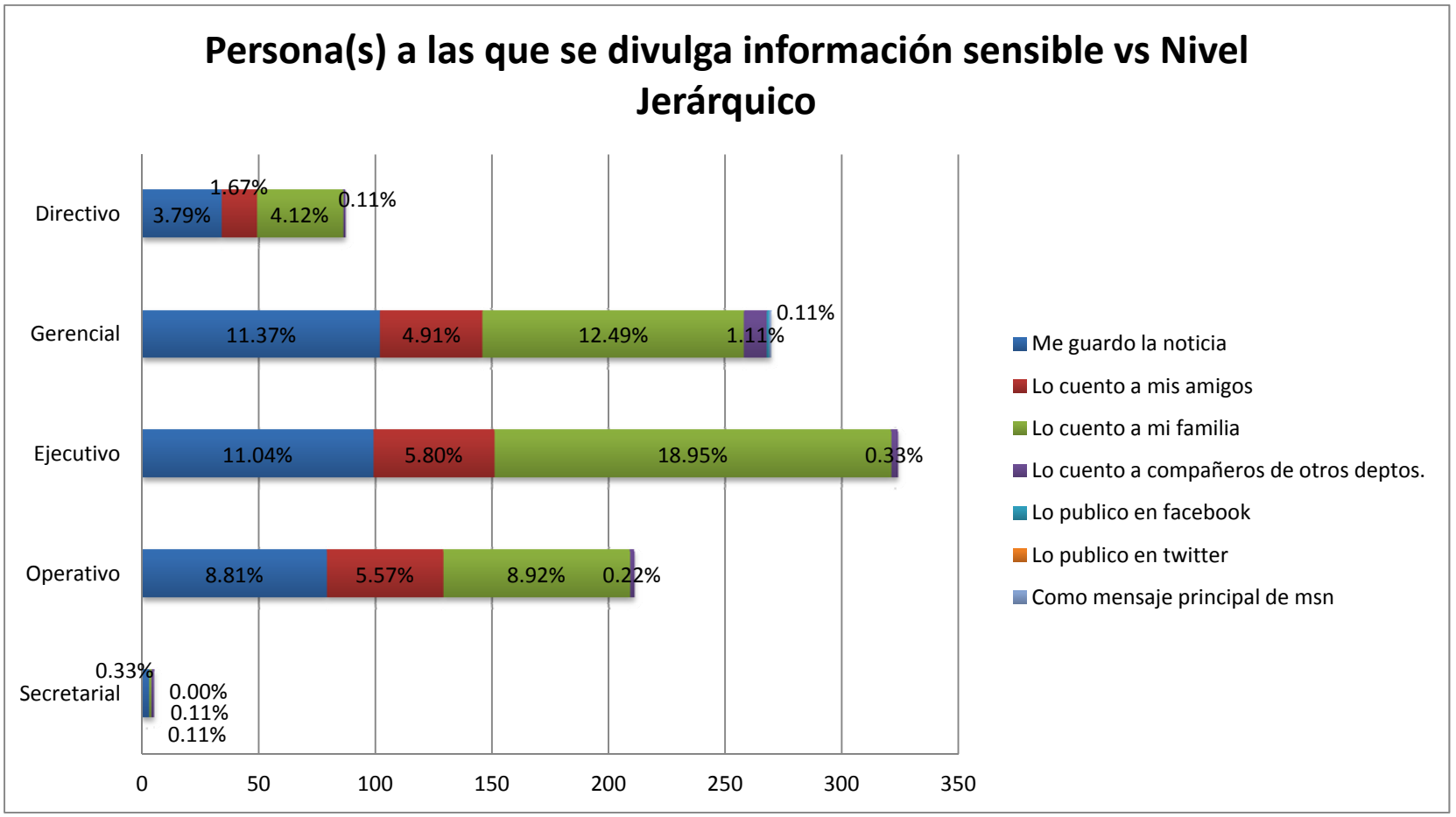
Interpretación: Con respecto a la correlación de los datos que se hizo referente al conocimiento o desconocimiento que los encuestados tienen respecto a otro de los ataques informáticos presentados con mayor frecuencia en el ámbito financiero "Phishing", se decidió correlacionar dicho dato con el último grado

de estudios con el que cuentan los empleados encuestados, esto con la finalidad de corroborar si el Grado de Estudios de los empleados encuestados tiene influencia en el conocimiento que se tiene de los ataques informáticos a los que están expuestos al hacer uso de un equipo de cómputo y/o comunicaciones.

De los datos arrojados en el gráfico se puede destacar que nuevamente, la barra en cuanto a desconocimiento excede en gran manera a la barra que refleja el conocimiento que tienen los empelados respecto al tema en cuestión. Aquellos empleados que afirmaron tener un conocimiento sólido respecto al ataque informático de tipo Phising y cuyo último grado de estudios es Licenciatura, se posiciona en primer lugar con un 6.35%; en segundo lugar destacan, con un 2.74%, los empleados que afirmaron conocer el ataque de tipo Pharming y cuyo máximo grado de estudos es la Maestría, y en tercer lugar se posiciona con un 1.72% los empleados que afirmaron conocer el ataque informático y que además su nivel de estudios es técnico.

Es interesante destacar que los porcentajes presentados en el gráfico que refiere al conocimiento del ataque infromático de tipo Phising se relaciona estrechamente con el gráfico presentado con antelación en el cual se expuso el conocimiento de los empleados respecto al ataque informático de tipo Pharming. Como se puede observar en ambos casos existe una menor incidencia por parte de los empleados que cuentan con nivel Doctorado; sin embargo, es importante resaltar que el número de empleados que cuenta con Doctorado, según datos estadísticos arrojados al principio de éste capítulo, es mucho menor al presentado para el nivel Licenciatura y Técnico.

De esto se puede concluir que si existe una correlación activa entre el último grado de estudios y el conocimiento que se tiene respecto al ataque informático de tipo Phishing; sin embargo, ésta es débil debido a que los porcentajes también se ven afectados con el número de empleados que labora en la institución y que según los datos arrojados en el capítulo anterior reflejaron un mayor índice de empleados cuyo grado de estudios representativo fue el nivel licenciatura y nivel Técnico. Asimismo, es importante resaltar la preocupación que existe al observar que un porcentaje mayor se vea reflejado en respuestas de un “total desconocimiento” por parte de los empelados respecto al tema, lo que podría propiciar que los trabajadores sean un blanco fácil ante ataques informáticos presentados, no sólo de éste tipo, sino de índole informático de manera general.



Interpretación: En un intento por conocer si la divulgación de la información sensible tiene influencia con el nivel jerárquico que ocupan los empleados de las instituciones de BM y de BM del Distrito Federal, dentro del sector financiero; se realizó la correlación de los datos correspondientes, los resultados fueron los siguientes.

Como se puede observar, el nivel Gerencial, seguido del nivel Ejecutivo, comparten el mayor porcentaje de los encuestados que señalan que ante una situación expuesta en la que reciben una noticia de índole confidencial, no divulgan fácilmente la información, esto se vio reflejado al momento de responder "Me guardo la noticia". De igual manera, se puede visualizar que en todos los niveles existe una mayor comunicación con la familia de los encuestados, a la cual se les comunica información respecto a las situaciones presentadas en el ámbito laboral, esto lo podemos observar en las barras de color verde y que aluden a la respuesta "Lo cuento a mi familia".

Por otro lado, respondiendo al cuestionamiento de la divulgación de información confidencial a otras personas externas y que no sea de índole familiar, se tiene que el nivel Gerencial y el nivel Ejecutivo presentan un porcentaje mayoritario en cuanto a la divulgación de información, reflejándose con el 6.13% cada uno respectivamente (4.91+1.11+0.11 y 5.80+0.33); cabe señalar que existe una mayor incidencia en el personal encuestado de nivel Ejecutivo que afirmó divulgar la información a sus amigos. Asimismo, el nivel directivo refleja un 1.78% (1.67+0.11) de los encuestados que afirmaron divulgar este tipo de información a terceros como amigos, gente de otro departamento de la institución, facebook, twitter y el messenger.

Finalmente, cabe señalar que, como se puede observar, existe una relación directa entre el nivel jerárquico y el tipo de información que se revela a terceros, sin embargo, esto no quiere decir que sea malo, sólo que hay que tener cuidado en qué tanta información se proporciona y de qué tipo es ésta, para evitar ser víctimas del uso malicioso de la información, lo que propiciaría que la institución quede expuesta y se atente contra la seguridad de su información.

CONCLUSIONES Y RECOMENDACIONES

En esta investigación se pudo constatar que la Ingeniería Social es una técnica que puede ser empleada de manera benéfica o maliciosa con el fin de obtener información de personas u organizaciones sin que éstas lo noten. Es por ello que las conclusiones obtenidas van acompañadas de recomendaciones entorno a la Seguridad de la información en las instituciones y el sector en estudio, así como en mejores prácticas en la Administración de la Tecnología.

Respondiendo a las preguntas de investigación se tiene que:

- La Ingeniería Social como medio de prevención y protección en la seguridad de la información de las instituciones de BM y de BD del sector financiero en el Distrito Federal, tiene bajo impacto debido a que los empleados en el sector tienen conocimientos escasos en la materia y en su aplicación; en consecuencia y desde el punto de vista de un posible ataque, el impacto es alto, lo que conlleva entre otros factores a una cultura endeble de seguridad generando pérdidas y fugas de información. La capacitación y difusión en este tema contribuiría en el fortalecimiento de la cultura de la seguridad de la información, ya que los empleados podrán y sabrán tomar las medidas pertinentes al momento de difundir información confidencial referente a la institución en la que laboran, o bien de índole personal.

- La relación que existe entre la seguridad de la información (SI), el hacking ético (HE) y la ingeniería social (IS) es sumamente estrecha, ya que la Ingeniería Social es una técnica que permite persuadir a las personas para que divulguen información de manera inconsciente, aledaño a ello se considera como parte de una auditoría de hacking ético en la cual se realiza lo mismo que un atacante haría, sin embargo, se hace con la finalidad de detectar los puntos vulnerables que pueden propiciar la fuga de información dentro de una institución. En relación con la seguridad de la información, la IS y el HE se convierten en una auditoría que en su conjunto ayudan a fortalecer la Seguridad de la Información de las instituciones.

- Existe un amplio desconocimiento, por parte de los empleados, respecto a los ataques informáticos a los que están expuestos al hacer uso de un equipo de cómputo y/o telecomunicaciones, tales como Phising, Pharming, entre otros. Esto es grave ya que coexiste una mayor susceptibilidad a ser víctima de ataques de éste tipo, lo que podría poner en riesgo la seguridad de la información de la institución. Para mermar este desconocimiento se recomienda realizar pláticas y conferencias respecto a las distintas vertientes que tienen los ataques informáticos, no sólo en el ámbito financiero, sino también de aquéllos cuya presencia es frecuente al hacer uso de los equipos de trabajo y personales.

- Los medios de comunicación que los empleados de las instituciones de BM y de BD acostumbran a utilizar para compartir información según su tipo son en su mayoría el uso del correo electrónico corporativo, la intranet y la forma impresa; sin embargo, también se vio reflejado el uso de la expresión oral de manera personal, así como el de otras aplicaciones tales como Share Point, Visual Source Safe, Microsoft Communicator, entre otras aprobadas por las instancias correspondientes. Esto no se considera como un foco de alerta alto; no obstante, se recomienda la implementación de métodos de seguridad en dichos medios de comunicación, con la finalidad de que la información

viaje de manera cifrada; así mismo, es recomendable que cuando los empleados se comuniquen de manera personal entre ellos, busquen el medio adecuado para hacerlo (oficina, sala de reunión, etcétera) debido a que cabe la posibilidad de que terceras personas se enteren de instrucciones o información de índole confidencial, cabe señalar que sería importante que ésta buena práctica se implementara como una política de la institución para evitar especulaciones por parte de los demás empleados.

De igual manera, es recomendable emplear servidores de correo que cuente con un protocolo de comunicación de tipo SSL (Secure Socket Layer) el cual proporciona un canal seguro y confiable por el cual la información viajará de manera segura evitando con ello que terceras personas puedan extraer dicha información a través de herramientas como los Sniffer. En lo que respecta al uso de celulares para el envío de mensajes de texto y el uso del teléfono institucional para llamadas telefónicas, es recomendable que la institución asegure que no exista intervención de línea telefónica o en su defecto podría hacer del conocimiento de los empleados que la información que comuniquen estos a través de la línea telefónica no sea de índole confidencial. Asimismo, como una muy buena alternativa para verificar la seguridad informática de la institución se recomienda la implementación de auditorías de hacking ético de manera periódica, con la finalidad de detectar puntos vulnerables que podrían ser mermados con antelación, evitando fugas de información sensible que podrían poner en riesgo la seguridad de la información de la institución.

- La edad no influye en la cultura de la seguridad de la información respecto a la Ingeniería Social, mientras que el nivel jerárquico y educativo si lo hacen.

- La Ingeniería Social es una técnica que puede contribuir a determinar la cultura de la seguridad de la información en instituciones de BM y de BD en el sector financiero; sin embargo, no lo es todo, para poder conocer la cultura de seguridad de la información con el que cuentan las instituciones en estudio, se requiere de una auditoría de Hacking Ético integral que contemple las distintas áreas a evaluar según el Manual de la Metodología Abierta de Testeo de Seguridad-OSSTMM 2.1, o bien otras metodologías propuestas y comprobables por instituciones afines al ámbito de la Seguridad Informática.

Con respecto a la hipótesis de trabajo planteada se concluye que:

- La hipótesis se cumplió parcialmente, ya que si bien es cierto que los empleados del sector en estudio mostraron tener conocimientos escasos respecto a la Ingeniería Social y por ende se deduce que son mayoritariamente susceptibles ante ataques de este tipo, que traen como consecuencia las fugas y pérdidas de información de la institución; no se pudo demostrar experimentalmente que dicha técnica impacta como medio de prevención y protección, debido a que ésta segunda parte se deja para fines de investigación en los que se aplique la técnica repetitivamente y se evalúen las diferencias presentadas en distintos periodos.

En lo que respecta al uso de redes sociales dentro de las instituciones de BM y de BD del Distrito Federal, cabe señalar que se tiene habilitado su acceso en las estaciones de trabajo de los empleados; sin embargo, el hecho de contar con acceso a las redes sociales no implica que esto sea malo, aunque si se recomienda hacer hincapié en los empleados para que tomen en consideración buenas prácticas en cuanto al uso de las mismas. Con esto, el uso cotidiano de las redes sociales no representará ningún riesgo, en cuanto a la fuga de información sensible, para las instituciones bancarias.

En lo referente a comentar acontecimientos ocurridos en el ámbito laboral a terceras personas como amistades y/o conocidos de otros departamentos o áreas de la institución, externos o desconocidos, el resultado es digno de tomarse en consideración ya que inclusive se hacen a través de redes sociales como Facebook y Twitter e incluso el Messenger. Éste es un foco de alerta para las instituciones bancarias, por lo que se recomienda concientizar a los empleados respecto al tipo de información que se expone de manera inconsciente referente a su ámbito laboral o personal. Asimismo, se recomienda verificar las políticas internas en este rubro y cotejarlas con los datos obtenidos en las preguntas 3 y 4 de la encuesta, esto debido a que se detectaron fugas de información de índole confidencial, tal como el desarrollo de nuevos proyectos de área o actividades específicas, lo que puede generar predisposición por parte de otros empleados, o bien que se difunda en áreas externas.

Por otra parte, cabe destacar que existe una población significativa de los encuestados que desconoce determinadas tecnologías de la información como lo es el Messenger y lo confunde con el correo electrónico. Para mitigar la falta de conocimiento respecto a las tecnologías de la información y Comunicación (TIC), principalmente en generaciones cuyas edades oscilan de los 45 años en adelante se recomienda fomentar conferencias, cursos o platicas referentes al uso de aplicaciones que funcionan como medios de comunicación tanto de manera síncrona como asíncrona y que podrían ser de uso frecuente en las instituciones bancarias.

Subsecuentemente, es importante destacar que las instituciones de BM y de BD, cuentan con políticas que señalan el cambio frecuente de las contraseñas, sin embargo, se tiene un porcentaje menor del personal que acostumbra a conservar la misma. Como recomendación a éste punto, se sugiere hacer mayor difusión a los empleados respecto a la importancia que tiene el cambio de contraseña de manera periódica.

Otro punto importante a señalar es que la mayoría de los empleados tienen una perspectiva favorable de la institución, con respecto al ámbito de la seguridad de la información; sin embargo, no se descarta la existencia de una pequeña porción de los encuestados que señalan lo contrario, incluso existe un índice considerable de los mismos que suelen comentar inconformidades respecto a su ámbito laboral a terceras personas. Esto es alarmante ya que la perspectiva que los empleados tienen respecto a la institución difiere en gran manera a la que la institución refleja ante los ojos de sus directivos u otros niveles jerárquicos de escalas mayores. Por ello se recomienda emplear un monitoreo constante, por medio de encuestas confidenciales aplicadas a los empleados, para conocer los motivos que propician que los trabajadores expresen esto y, por supuesto, tomarlos en consideración para posibles mejoras en las instituciones.

Respecto a experiencias frutos de esta investigación se concluye lo siguiente:

- La relación que tuvo este trabajo de investigación respecto a la Maestría en Administración de la Tecnología es muy extensa, ya que permitió aplicar los conocimientos adquiridos a lo largo de mi estancia en la Maestría que me sirvieron de apoyo y contribuyeron en gran manera para la complementación de dicha investigación.

- A cada una de las instituciones que me permitió aplicar el instrumento correspondiente se les proporcionó, independientemente de este estudio, un informe con la evaluación respectiva de los resultados obtenidos a raíz de las encuestas aplicadas en su institución. Aunado a ello, cabe señalar que se realizaron entrevistas previas con algunos de los directivos de las instituciones en estudio, entrevistas en las que se expresó su perspectiva respecto a la cultura de seguridad de la información que consideraban que sus empleados tenían, evaluándola como alta; sin embargo, recordemos que la Ingeniería Social sólo es parte de ese conjunto para conocer la cultura de seguridad de la información de los empleados, y respecto a éste ámbito, los resultados arrojados muestran que se tiene un desconocimiento respecto al tema por lo que se es más susceptible a fugas y robo de información.

- Para la aplicación de la encuesta y para efectos legales se realizaron acuerdos de confidencialidad y derechos de autor que se establecieron por escrito para asegurar la confidencialidad de los resultados de las instituciones respectivas, sin embargo,

- Existieron muchas dificultades para poder aplicar el instrumento debido a situaciones de logística por parte de las personas que fueron asignadas para dar seguimiento a la petición del estudio. Asimismo, en algunos casos la obstrucción se dio debido a las políticas sustentadas por las instituciones correspondientes, o bien por parte del área de seguridad y sistemas de las mismas.

- En la mayoría de los casos se presentó una gran disponibilidad de participación por parte de los Directivos Generales de cada una de las instituciones bancarias; sin embargo, a nivel Secretarial surgieron constantes excusas en cuanto a la posible aplicación de la encuesta por medio de vía web. Se planteó la posibilidad de aplicar el instrumento de manera impresa a los empleados, sin embargo, no hubo respuesta positiva por parte de los encomendados para llevar a cabo el seguimiento de dicho estudio.

- Aún existe un temor latente respecto al tema del Hacking debido a que en algunas instituciones, al momento de presentarles la propuesta del instrumento de la investigación, exponiendo que la Ingeniería Social es una técnica derivada de una auditoría integral de Hacking ético, rechazaron tajantemente la aplicación del mismo.

- El Hacking Ético es poco conocido en el ámbito financiero, y por ende existe un rechazo latente al mismo.

Finalmente, invito a las instituciones de BM y de BD a que tomen como referencia este trabajo de investigación y consideren una amplia difusión en cuanto al conocimiento y aplicación de la Ingeniería Social y los ataques informáticos a los que se puede ser susceptible en el campo laboral del sector financiero, difundiendo una cultura de seguridad de la información a todas las áreas de las instituciones. Esto con la finalidad de mermar en gran manera los puntos vulnerables y proteger de manera fiable la información confidencial de las instituciones, logrando así una organización mayoritariamente confiable y fidedigna que traerá como consecuencia grandes logros que se verán reflejados en el progreso de las instituciones y la seguridad de la información.

BIBLIOGRAFÍA

- Aceituno, V. (2006). *Seguridad de la información: Expectativas, riesgos y técnicas de protección.* México: Limusa.
- Adler Lomnitz, Larissa (2002). Redes sociales y partidos políticos en Chile. Revista hispana para el análisis de redes sociales. 3(2). Recuperado el 02 de octubre de 2011 de la base de datos RedIRIS.
- Alvy (2002). Malos usos de la Ingeniería Social. La información.com. Recuperado el 21 de noviembre de 2011 en http://www.microsiervos.com/archivo/seguridad/mala-ingenieria-social.html
- Anonymous (2010). A*rm yourself against Black Hats.* E-World. Recuperado el 11 de noviembre de 2010 de la base de datos Businessline. Business Law Today
- Arcos, Sergio. (2011). *Ingeniería social: Psicología aplicada a la seguridad informática*. Tesis de Licenciatura. Ingeniería de Servicios y Sistemas de Información (ESSI).
- Autor Desconocido (2009). Hacking Ético: Seguridad Informática. Prospectivas Tecnológicas. Recuperado el 19 de noviembre de 2011 en http://prospectivas-tecnologicas-xxi.blogspot.mx/2009/09/hacking-etico.html
- Autor desconocido (2009). La Ingeniería Social evoluciona. News PCS asycom. Recuperado el 29 de abril de 2012 en http://www.newspcs.com/6143/la-ingenieria-social-evoluciona.html
- Blog Tecnológico (2009). La ingeniería social se traslada de los chats a las redes sociales. Recuperado el 10 de diciembre de 2011 en http://www.blogtecnologico.net/ingenieria-social-traslada-redes-sociales/
- Britt, Phillip. (2005). Ethical Hackers: Testing the Security Waters. *Information Today* .22(8), 1-2. Recuperado el 15 de noviembre del 2010 de la base de datos Web of Knowledge.
- Caballero, Oscar (2009). Ingeniería Social "Phishing". Recuperado el 20 de noviembre de 2011 en http://sitioconfiable.blogspot.mx/
- Ciemencia, Jaime (1982). Diferencias Motivacionales según el nivel jerárquico en entidades financieras de servicio. *Revista Latinoamericana de Psicología.* 14(1).
- CNBV Comisión Nacional Bancaria y de Valores (2012). Instituciones que conforman la Banca Múltiple y la Banca de Desarrollo en México. Consultada el 15 de julio del 2011 en http://www.cnbv.gob.mx/Paginas/Index.aspx
- Coffin, Bill. (2003). IT takes a thief: Ethical hackers test your defenses. *Risk Managemen.* 50(7), 10. Recuperado el 15 de noviembre del 2010 de la base de datos Web of Knowledge.

- Daltabuit, E. et. al. (2007). *Seguridad de la información.* Noriega, México: Limusa

- Deloitte (2010). Informe anual de Seguridad en Entidades Financieras. Auditoría Fiscal y Legal. Consultoría. Asesoramiento Financiero.

- Deloitte (2009). Informe anual de Seguridad en Entidades Financieras. Auditoría Fiscal y Legal. Consultoría. Asesoramiento Financiero.

- Departamento de Planeamiento y Desarrollo (2011). Plan Estratégico. Banco de la Nación 2009 – 2013. Recuperado de la base de datos del Banco de la Nación de la República del Perú.

- Desconocido (2010). Infome Anual de Seguridad en Entidades Financieras. Profesionaleshoy. Recuperado el 15 de diciembre de 2012 en http://profesionaleshoy.es/informe-anual-de-seguridad-en-entidades-financieras/29/09/2010

- Dragonjar (2012). The Social-Engineer Toolkit. Recuperado el 29 de abril de 2012 en http://www.dragonjar.org/the-social-engineer-toolkit.xhtml

- ESET (2011). Guía de Seguridad para el uso adecuado de las redes sociales. Paperblog. Recuperado el 26 de abril de 2012 en http://es.paperblog.com/guia-de-seguridad-para-el-uso-adecuado-de-las-redes-sociales-644917/

- Gartner Research (2011). Social Engineering: Exposing the Danger Within. Gartner. 1(1).

- González, María (2002). El sistema financiero mexicano. El entorno Financiero y los mercados.Gestiopolis.com

- Goodwin, Bill. (2006). Ethical hacking on rise. *Computer Weekly.* 8. Recuperado el 14 de noviembre del 2010 de la base de datos Web of Knowledge.

- Granger, Sarah (2010). Social Engineering reloaded. Symantec. Recuperado el 10 de julio de 2011 en http://www.symantec.com/connect/articles/social-engineering-reloaded

- Guenther, Melissa (2001). Social Engineering- Fact or Fallacy? Fortune Magazine. Security Awareness Series.

- Harris, S. et. al. (2005). *Hacking ético. Traducción de: Gray Hat Hacking.* Madrid: Anaya Multimedia.

- Hasan, Mosin (2010). Case study on social engineering techniques for persuasion. International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC). 2(2).

- Herzog, Pete (2003). "OSSTMM 2.1 Manual de la Metodología Abierta de Testeo de Seguridad. USA: ISECOM Institute for Security and Open Methodologies. Recuperado el 30 de septiembre de 2010, http://www.isecom.org/research/osstmm.html

- Hinson, Gary (2008). Social Engineering Techniques, Risks, and Controls. EDPACS: The EDP Audit, Control, and Security Newsletter.37(4-5), 32-36. Recuperado el 30 de septiembre de 2011 en http://www.tandfonline.com/doi/abs/10.1080/07366980801907540

- Iregui V., Luis Andrés (2010). Internet Explorer, el navegador más seguro contra la ingeniería social. Enter.co.

- Iregui V., Luis Andrés (2010). 10 mandamientos para mejorar su seguridad informática (DISI 2010). Enter.co.

- Kotadia, Munir (2004).Greates Security Risk:Social Engineering. ZDNet UK Recuperado el 25 de septiembre de 2011 en http://www.social-engineer.org/wiki/archives/SEDefined/SEDefined-GreatestRisk.htm

- Loreto, Vicente. (2004). ¿Movimientos sociales en la red? Los hacktivistas. *El Cotidiano, Universidad Autónoma Metropolitana-Azcapotzalco.* 20(126). Recuperado el 15 de noviembre del 2010 de la base de datos Web of Knowledge.

- Martínez Aguirre, Tania Guadalupe (2009). *Seguridad en el acceso a los sistemas de información.* Tesis de Licenciatura. Universidad Lasallista Benavente.

- Mexis. Seguridad Administrada (2009). Compañía experta en seguridad y redes de datos. México. Recuperado el 29 de abril de 2012 en http://www.mexis.net/

- Mexis (2009). Sector Financiero y TI: Seguridad ante todo. Mexis Seguridad Administrada. Recuperado el 24 de noviembre de 2011 en http://www.mexis.net/pdf/wp-financiero.pdf

- Microsoft, pymes y autónomos (2011). Qué son y cómo funcionan las Redes Sociales. Artículos y recursos empresariales. Recuperado el 12 de octubre de 2011 en http://www.microsoft.com/business/es-es/Content/Paginas/article.aspx?cbcid=71

- Mieres, Jorge (2009). Ataques Informáticos. Debilidades de Seguridad comúnmente explotadas. México: Evil Fingers White paper.

- Mitnick, Kevin. (2002). *Controlling the Human Element of Security. The Art Of Deception*. USA: .John Wiley & Sons Australia.

- Open Source Community and Rapid7 (2012). Metasploit. USA. Recuperado el 29 de abril de 2012 en http://www.metasploit.com

- OWASP Foundation (2008). Guía de pruebas OWASP versión 3.0. USA: OWASP The open Web Application Security Project. Recuperado el 29 de abril de 2012, https://www.owasp.org/index.php/Category:OWASP_Testing_Project

- Picouto, F. et. al. (2004). *Hacking práctico.* España: Anaya Multimedia.

- Raether, Ronald I Jr. (2008). DATA SECURITY AND ETHICAL HACKING: Points to Consider for Eliminating Avoidable Exposure*. Business Law Today*, 18(1). 55. Recuperado el 14 de noviembre del 2010 de la base de datos Web of Knowledge.

- Ramos, Daniel (2004). Aplicación de herramientas tecnológicas a los servicios financieros. Gestiopolis.com

- Rodríguez, L. A. (1995). *Seguridad de la información en sistemas de cómputo.* México D.F: Ventura.

- Rodríguez, Margarita (2004). L*a influencia de la cultura organizacional en la implantación de la estrategia de seguridad de la información en una organización financiera*. Tesis de Maestría. Universidad Iberoamericana Santa Fé.

- Sandoval, Hugo (2008). Movilidad 2.0. InformatioWeek. Recuperado de la base de datos de InformationWeek Mexico.

- Segu-Info (2011). Crecimiento de la Ingeniería Social en las Redes Sociales. Segu.Info News. Noticias sobre Seguridad de la Información. Recuperado el 12 de diciembre de 2011 en http://blog.segu-info.com.ar/2011/08/crecimiento-de-la-ingenieria-social-en.html#ixzz1tUHmMCeK

- Social Engineering Framework (2011). Social Engineering. Recuperado el 14 de septiembre de 2011 en http://www.social-engineering.org/se-resources/

- Sophos (2008). *La banca se blinda: nuevas tendencias en seguridad informática*. Sophos. Recuperado el 10 de dicembre de 2011 en http://www.sophos.com/es-es/press-office/press-releases/2008/10/la-banca-se-blinda.aspx

- Scott, Spencer (2011). Ingeniería Social: eludiendo el "firewall humano". Revista Virtual Magazcitum.

- Sportsman, Nathan (2011). Social Engineering. Recuperado el 13 de septiembre de 2011 en http://www.slideshare.net/praetorianlabs/praetorian-social-engineeringpresentation

- Universidad Columbia del Paraguay (2011). *Universidad que imparte la carrera de la Ingeniería Social*. Recuperado el 10 de noviembre de 2010 de http://webcache.googleusercontent.com/search?q=cache:JMVP3Kj7dakJ:www.columbia.edu.py/carreras-is.html+investigaciones+de+ingenier%C3%ADa+social&cd=3&hl=es&ct=clnk&gl=mx&client=firefox-ac

- Winkler, Ira (1996). Case study of industrial espionage through social engineering. National Computer Security Association.

- Zorrilla, Juan P. (2004). La importancia de las pymes en México y para el mundo. GestioPolis. Recuperado el 29 de abril de 2012 en http://www.gestiopolis.com/canales2/economia/pymmex.htm

ANEXOS

ANEXO 1. INSTRUMENTO DE ESTUDIO REALIZADO 1

```
CREATE TABLE IF NOT EXISTS `data` (
  `ip` int(11) NOT NULL,
  `1` int(2) NOT NULL,
  `2` int(2) NOT NULL,
  `3` int(2) NOT NULL,
  `4` int(2) NOT NULL,
  `5` int(2) NOT NULL,
  `6` int(2) NOT NULL,
  `7` int(2) NOT NULL,
  `A` int(2) NOT NULL,
  `B` int(2) NOT NULL,
  `C` int(2) NOT NULL,
  `D` int(2) NOT NULL,
  `E` int(2) NOT NULL,
  PRIMARY KEY (`ip`)
) ENGINE=MyISAM DEFAULT CHARSET=latin1;
```

~/www/index.html

```
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN"
"http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
<html><head><title>WebSort [facebook]</title>
<meta http-equiv="Content-Type" content="text/html; charset=utf-8" />

<link rel="stylesheet" type="text/css" href="encuesta.css">
<script type="text/javascript">
var count = 0;
var str = "";
function writeText(txt)
{
    var map = document.getElementById("map")
    var id  = document.getElementById(txt);
    map.removeChild(id);
    document.getElementById("desc").innerHTML =
document.getElementById("desc").innerHTML+" "+txt;
    str = str + txt;
    count++;
    if (count==12) {
        showExit();
    }
}
function showExit() {
    document.location="recogerDatos.php?s="+str;
}
function showDialog() {
    document.getElementById("dialog").style.display = 'block'
}
function closeDialog() {
    document.getElementById("dialog").style.display = 'none'
}
```



```
</script>
</head>
<body onLoad="showDialog();">
<div id="dialog">
<h1>WebSort de Facebook</h1>
<p>Has llegado a la página web de Sergio Arcos, un estudiante de
Ingeniería
informática realizando su Proyecto Final de Carrera.</p>
<p>Me gustaría invitarte a contribuir en este realizando una pequeña
actividad. Serán apenás 5 minutos.</p>
<h2>¿Qué debo hacer?</h2>
<p>En la siguiente pantalla te vas a encontrar una imagen representando
una
cuenta ajena de Facebook. En ella hay 12 carácteres, divididos en 7
números y 5
letras.</p>
<p>Los números representan los elementos comunes en casi cualquier
pantalla.</p>
<p>Las letras son las páginas internas de Facebook donde puedes
navegar.</p>
<p>Aún así, no le prestes atención a esto, sólo es orientativo.</p>
<br />
```

```
<p>Te pido lo siguiente: Imagina que acabas de conocer a esta persona y
te
ha dado curiosidad por mirar su perfil. Bien,</p>
<h2>¿De dónde sacarías la información para preguntarle sobre él?</h2>
<p>Debes seleccionar en orden de "primero" (más importante) a "último"
(menos importante) los 12 elementos que hay (con un click encima
basta).</p>
<p>Te pido que te metas profundamente en el papel de "pícaro" y
visualices
esta imagen como si fuera un caso real (imagina donde clickarias en la
cuenta
de tu mejor amigo o amiga).</p>
<p>Tomate tu tiempo, o hazlo bien rápido. Se natural. (Si ves que lo has
hecho mal, termina la encuesta y vuelve a esta página: puedes volver a
rellenarla).</p>
<a href="javascript:closeDialog();">EMPEZAR</a>
</div>
<img src="facebook.png" width="996" height="768" alt="[facebook_map]"
usemap="#fbmap" />
<map id="map" name="fbmap">
<area id="1" shape="rect" coords="0,65,189,204"
href="javascript:writeText('1');" alt="[foto de perfil]" />
<area id="2" shape="rect" coords="0,325,189,418"
href="javascript:writeText('2');" alt="[relacion]" />
<area id="3" shape="rect" coords="0,418,189,574"
href="javascript:writeText('3');" alt="[amistades]" />
<area id="4" shape="rect" coords="0,574,189,768"
href="javascript:writeText('4');" alt="[familia]" />
<area id="5" shape="rect" coords="189,65,701,136"
href="javascript:writeText('5');" alt="[datos personales]" />
<area id="6" shape="rect" coords="189,137,701,204"
href="javascript:writeText('6');" alt="[previsualizacion de fotos]" />
<area id="7" shape="rect" coords="723,137,967,204"
href="javascript:writeText('7');" alt="[relacion tu y yo]" />
<area id="A" shape="rect" coords="278,263,511,368"
href="javascript:writeText('A');" alt="[pagina muro]" />
<area id="B" shape="rect" coords="278,394,511,537"
href="javascript:writeText('B');" alt="[pagina informacion]" />
<area id="C" shape="rect" coords="598,259,830,484"
href="javascript:writeText('C');" alt="[pagina imagenes]" />
<area id="D" shape="rect" coords="278,556,511,709"
href="javascript:writeText('D');" alt="[pagina canciones]" />
<area id="E" shape="rect" coords="598,505,830,724"
href="javascript:writeText('E');" alt="[pagina amigos]" />
</map>

              <p id="desc"></p> </body></html></body></html>
```

~/www/recogerDatos.php

```
<?php

function insertValues() {
    if (!isset($_GET['s'])) {
        return false;
    }

    $ip = ip2long($_SERVER['REMOTE_ADDR']);
    $s = strtoupper($_GET['s']);

    if (strlen($s)!=12) {
        return false;
    }

    $arr = array();
    $check = array('1','2','3','4','5','6','7','A','B','C','D','E');

    for ($i=0; $i<12; $i++) {
        $pos = strpos($s,$check[$i]);
        if ($pos === false) return false;
        $arr[$i] = 12-$pos;
    }

    $db = mysql_connect('localhost', '266474_websort', 'websort.');
    mysql_select_db('martes_zxq_websort', $db);


    $R = mysql_query("INSERT INTO `data` (
    `ip`,
    `1`, `2`, `3`, `4`, `5`, `6`, `7`,
    `A`, `B`, `C`, `D`, `E` )
    VALUES (
        $ip,
        '$arr[0]','$arr[1]','$arr[2]','$arr[3]','$arr[4]','$arr[5]','$arr[6]',
        '$arr[7]','$arr[8]','$arr[9]','$arr[10]','$arr[11]'
    )
    ON DUPLICATE KEY UPDATE
    `1`='$arr[0]', `2`='$arr[1]', `3`='$arr[2]', `4`='$arr[3]',
    `5`='$arr[4]', `6`='$arr[5]', `7`='$arr[6]', `A`='$arr[7]',
    `B`='$arr[8]', `C`='$arr[9]', `D`='$arr[10]', `E`='$arr[11]'", $db);

    // echo mysql_error();

    return true;
}
```

```
if (insertValues()) {
    require("ok.html");
} else {
    header("location: index.html");
}
?>
```

~/www/analyze.r

```
## dd = datos registrados
dd     <-     read.table("facebook.dat",
header=T, sep=" ")
dd <- dd[2:13]
dm <- dd
dd                                        <-
data.frame(sum(dd[1]),sum(dd[2]),sum(dd
[3]),sum(dd[4]),sum(dd[5]),sum(dd[6]),s
um(dd[7]),sum(dd[8]),sum(dd[9]),sum(dd[
10]),sum(dd[11]),sum(dd[12]))

## dm = datos registrados - el máximo

##     dt     =     analisis     evaluado
"objetivamente"
dt   <-   read.table("facebookTres.dat",
header=T, sep=" ")


dd <- 100*(dd/sum(dd))
dt <- 100*(dt/sum(dt))
colnames(dd) <- colnames(dt)

ncon <- ncol(dm)
for (i in 1:ncon) {
    dm[i] <- nrow(dm[dm[i]==12,])
}
dm = dm[1,]
dm <- 100*(dm/sum(dm))



barplot(as.matrix(dd),     ylim=c(0,50),
main="Datos          en          crudo",
xlab="Divisiones", ylab="Porcentaje")
barplot(as.matrix(dm),     ylim=c(0,50),
main="Vistas      SUBJETIVAMENTE      más
vulnerables",          xlab="Divisiones",
ylab="Porcentaje")
barplot(as.matrix(dt),     ylim=c(0,50),
main="Vistas      OBJETIVAMENTE      más
vulnerables",          xlab="Divisiones",
ylab="Porcentaje")
```

```
n                                         <-
matrix(as.matrix(rbind(dm,dt)),ncol=12)

colnames(n)<-colnames(dd)
rownames(n)<-c("sub","obj")

n <- as.table(n)
ns <- n[ , order(n[2,])]

barplot(ns,                  ylim=c(0,50),
legend.text=c("Información
subjetiva","Información      objetiva"),
main="Subjetividad    vs    Objetividad",
xlab="Divisiones",    ylab="Porcentaje",
beside=T)




## Gráfico de localizaciones
loc     <-     read.table("location.dat",
header=T, sep=" ")

plot(loc,     main="Paises     de     los
parcipantes",       legend.text=c("77.6%
españoles",        "22.4%        resto"),
xlab="Pais",ylab="N°                    de
participantes" )

pie(loc)
```

Regresar a estudio realizado 1

ANEXO 2. INSTRUMENTO DE ESTUDIO REALIZADO 2

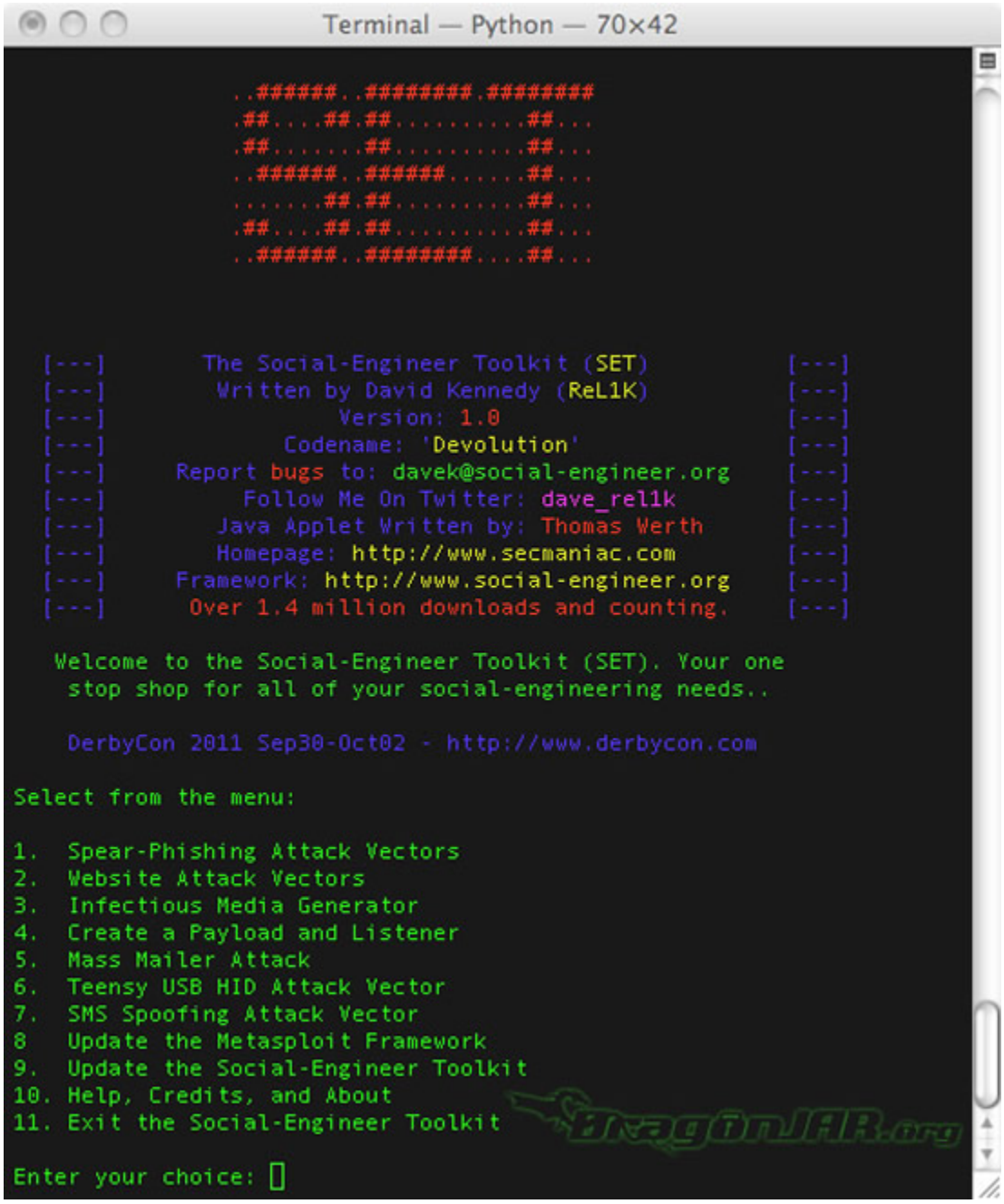
Actualizado:

Acaba de salir una nueva versión 1.1 del Social-Engineer Toolkit con nombre clave "Happy Holidays", en la que se incorporan las siguientes novedades:

- Cuatro nuevos Client-Side Attacks basados en Metasploit
- Optimizaron el servidor Web, los multihilos que manejaba y mejoraron algunas funcionalidades del código, para acelerar su funcionamiento
- Nueva opción set_config con la que podrás especificar si deseas o no redireccionar automáticamente por ejemplo a un applet de java en un ataque múltiple del tipo Applet Java+ Credential Harvester de esta forma solo se redireccionará al applet de Java si la credencial fue aceptada.
- Se añadió soporte para UPX

Iniciando el The Social-Engineer Toolkit

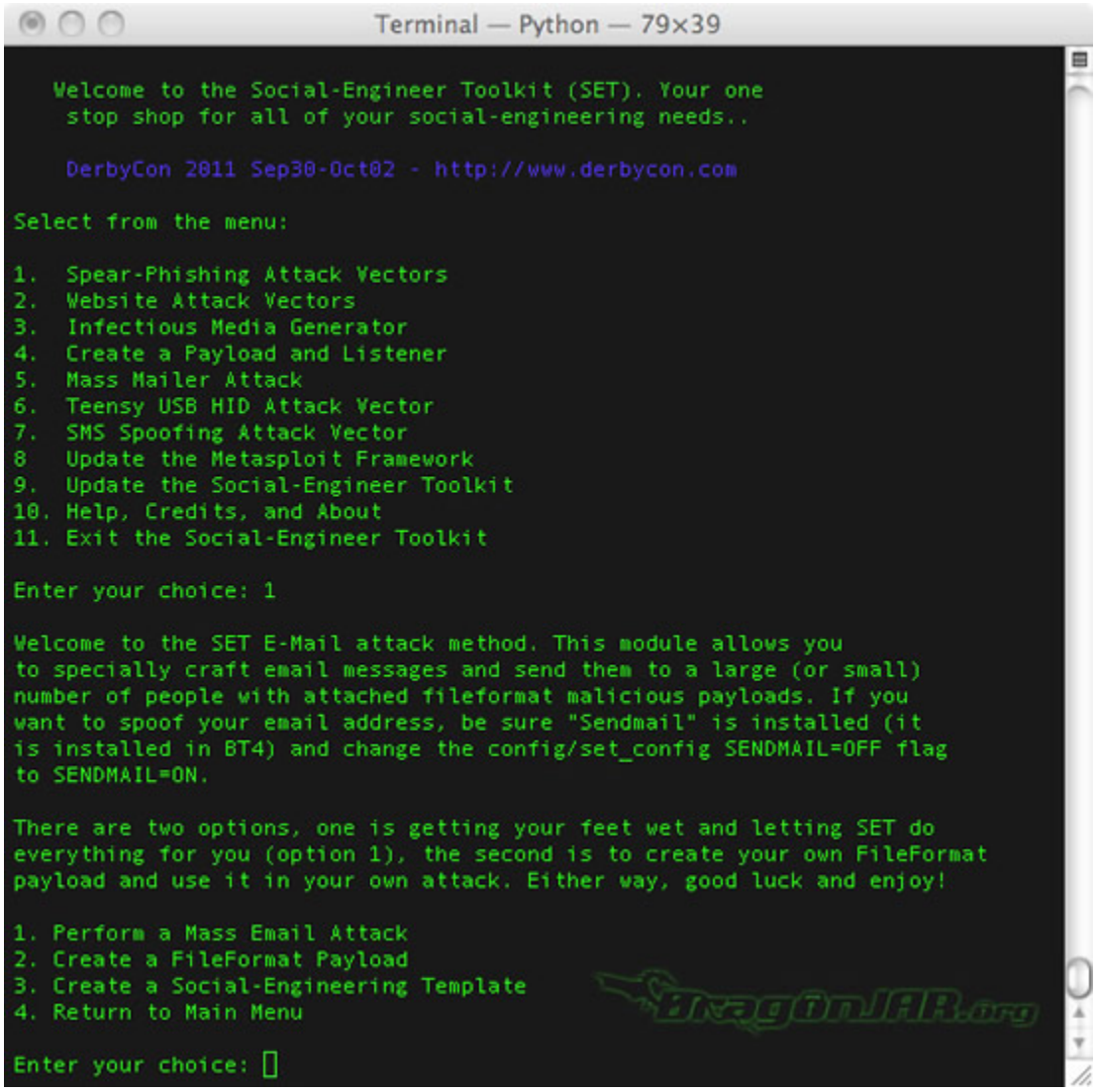
SET es multiplataforma, y solo necesitamos tener instalado el interprete de Python para ejecutarlo y ejecutarlo con **./set** o ***Python set*** en la carpeta donde lo tengamos guardado (las dependencias que no tengas, las descargará automáticamente).



Al iniciar el SET, lo primero que vemos es un menú que nos ofrece una gran cantidad de opciones para lanzar nuestro ataque de ingeniería social, desde la creación de correos fraudulentos, paginas que al visitarlas infecta tu maquina, archivos multimedia que permite obtener acceso al equipo de la víctima, la posibilidad de enviar correo masivo, crear un CD/DVD o memoria USB que infecte la maquina y hasta enviar mensajes de texto que nos ayude en nuestra tarea.

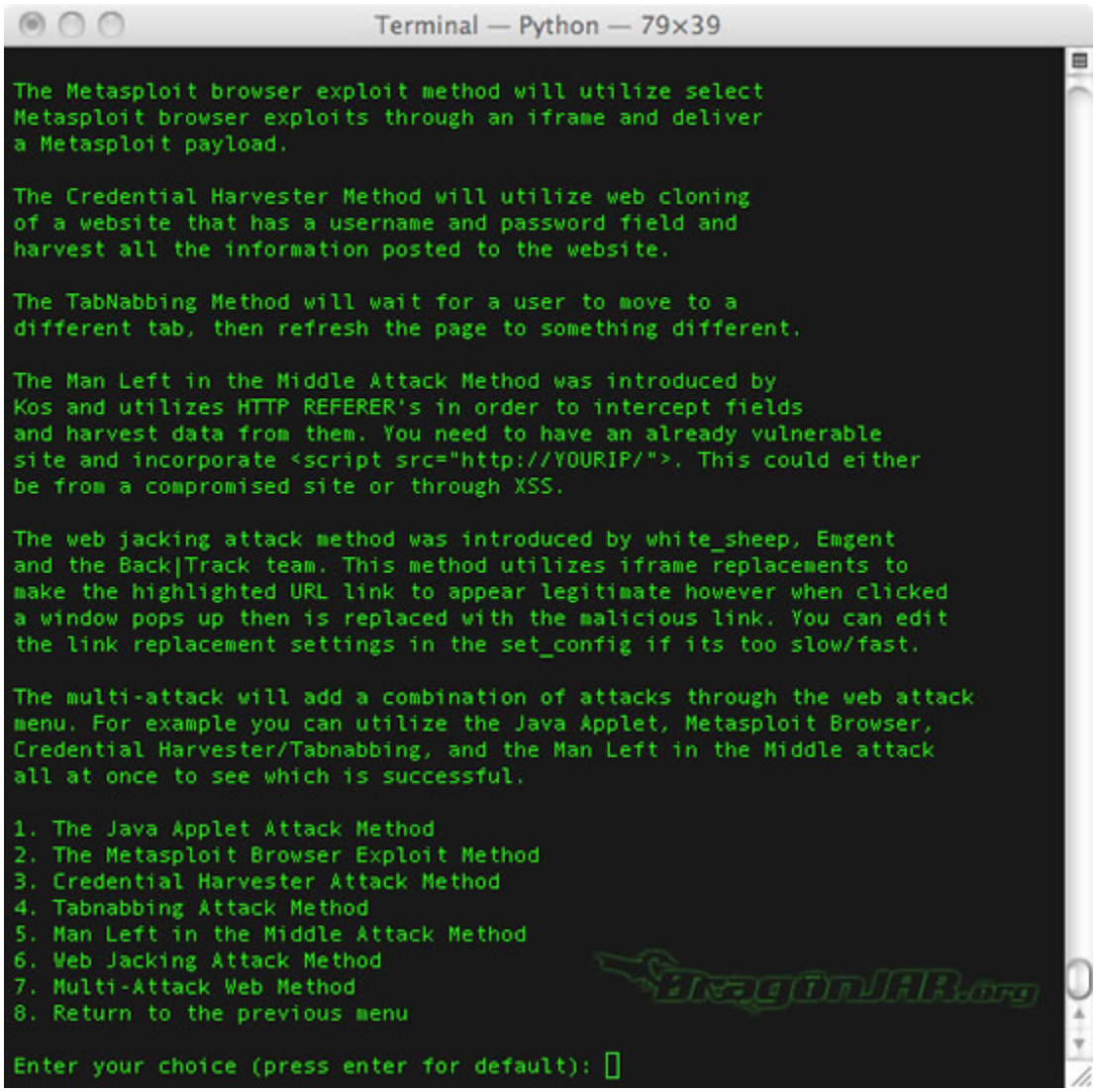
Sistema de Phishing en el The Social-Engineer Toolkit

El sistema de creación de phishing en el SET es bastante completo, nos permite generar automáticamente un sitio falso con el cual engañar a los destinatarios o enviar de forma masiva correos con adjuntos maliciosos que permiten el acceso remoto de su máquina.



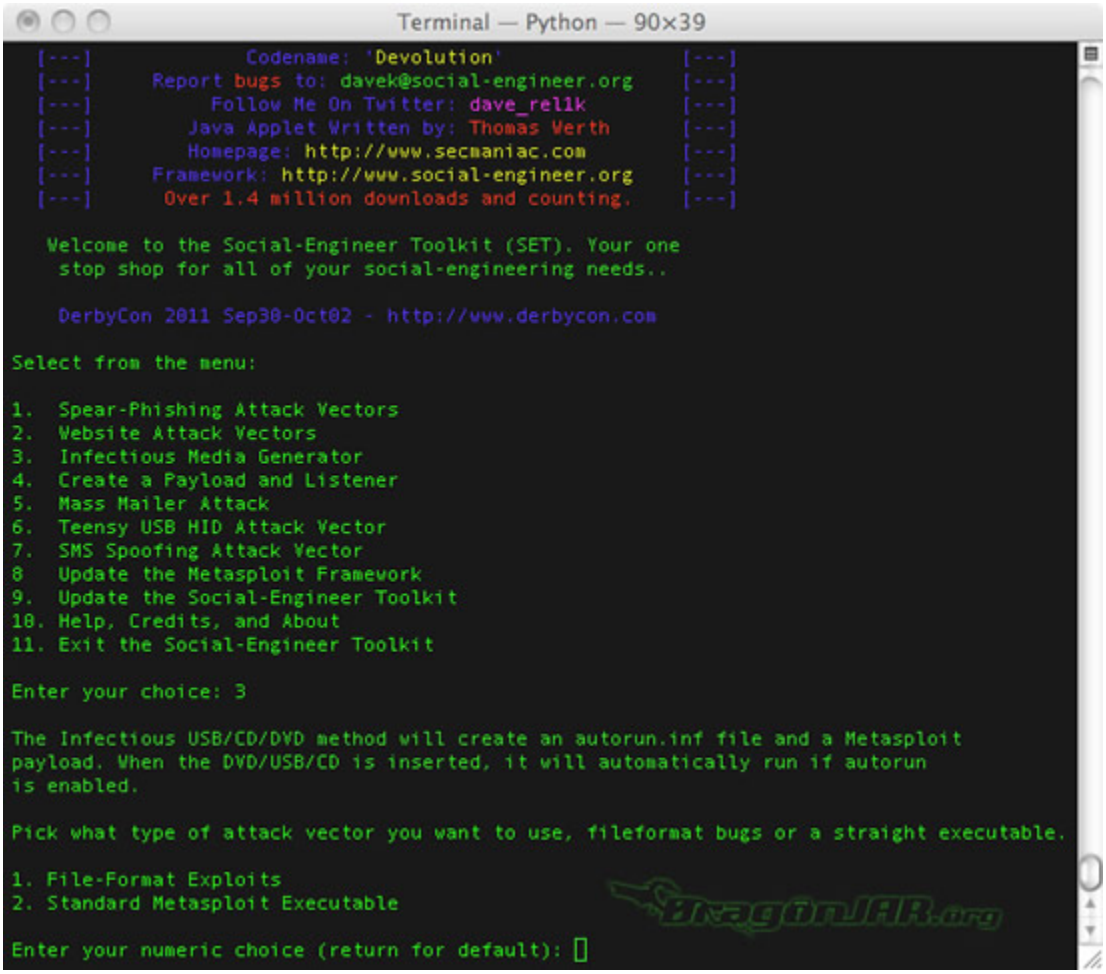
Vector de Ataque Web en el The Social-Engineer Toolkit

SET también permite realizar ataques automáticos a un usuarios que ingrese (por medio de ingeniería social) a una dirección que tu le especifiques (ahora lograr esto es mucho más fácil gracias a los acortadores de direcciones), SET se encarga de subir el servidor y realizar el ataque que le especifiques (un applet de java, ataques múltiples, o tabnabbing , entre otros) que te devolverá una shell en el equipo víctima.



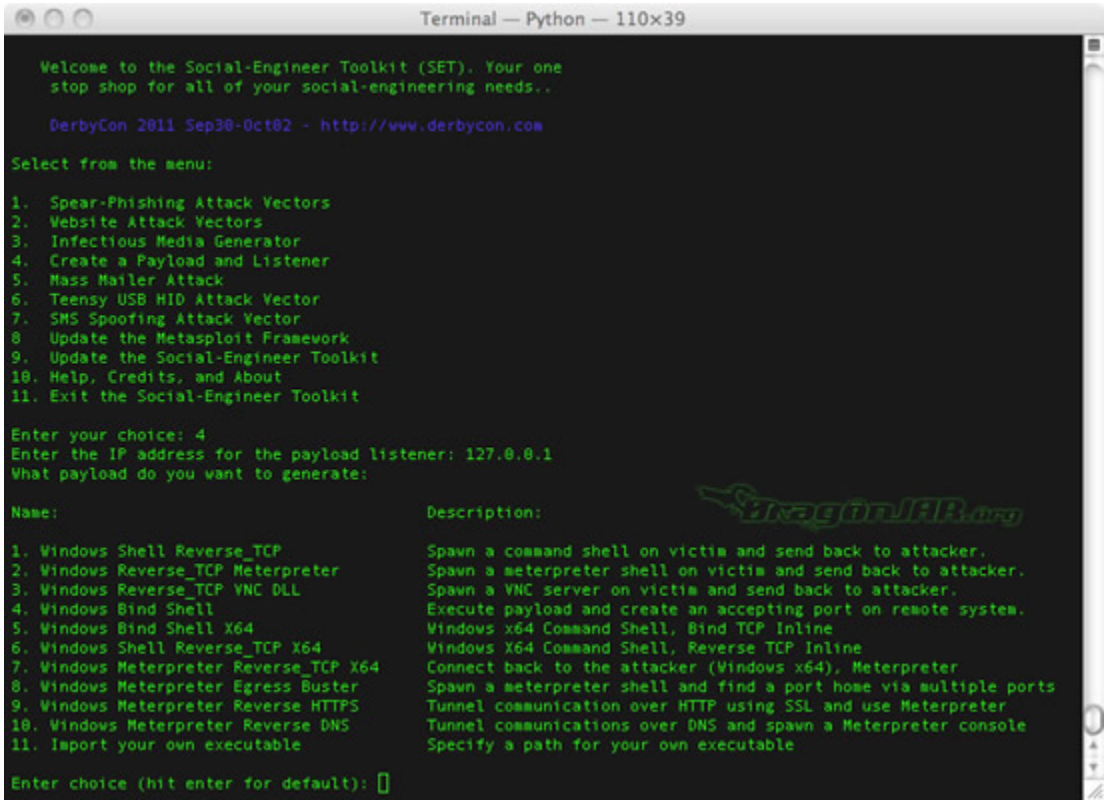
Creación de Medios Infectados en el The Social-Engineer Toolkit

Permite crear un archivo que se conecte remotamente a nuestra maquina, ofreciéndonos una shell del sistema y se ejecute en el equipo remoto al introducirse una memoria/disco duro USB, o un disco DVD/CD aprovechando el "autorun" de windows.



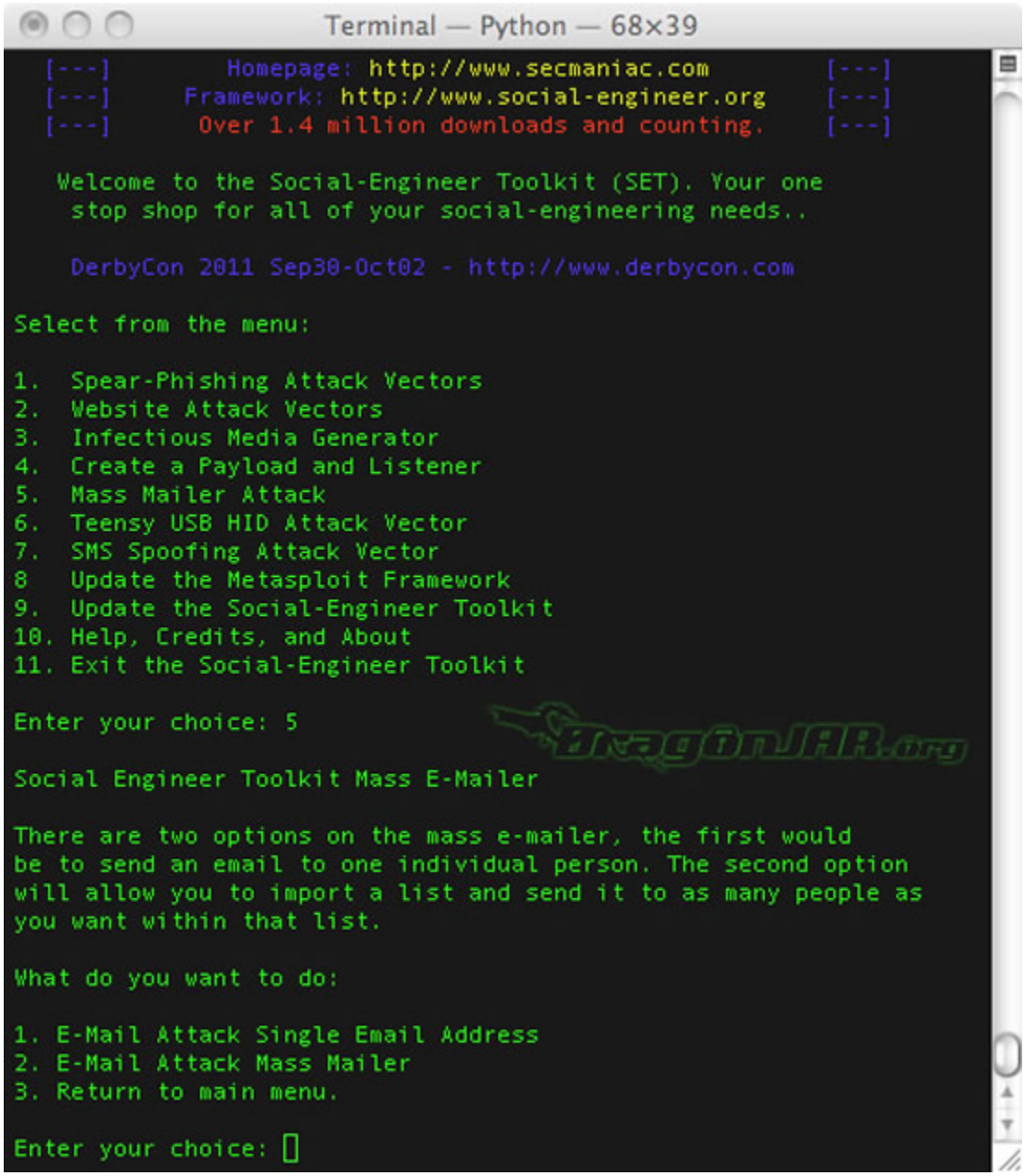
Generar ejecutable con Payload en el The Social-Engineer Toolkit

SET también permite (con la ayuda de metasploit framework) generar un ejecutable que se conecte remotamente a nuestra maquina, una vez lo abran en la maquina víctima, permitiéndonos configurar una gran cantidad de shells, entre ellas la famosa meterpreter, shells ciegas de windows, shells remotas y todo esto para procesadores a 32 y 64Bits



Ataques por Correo en The Social-Engineer Toolkit

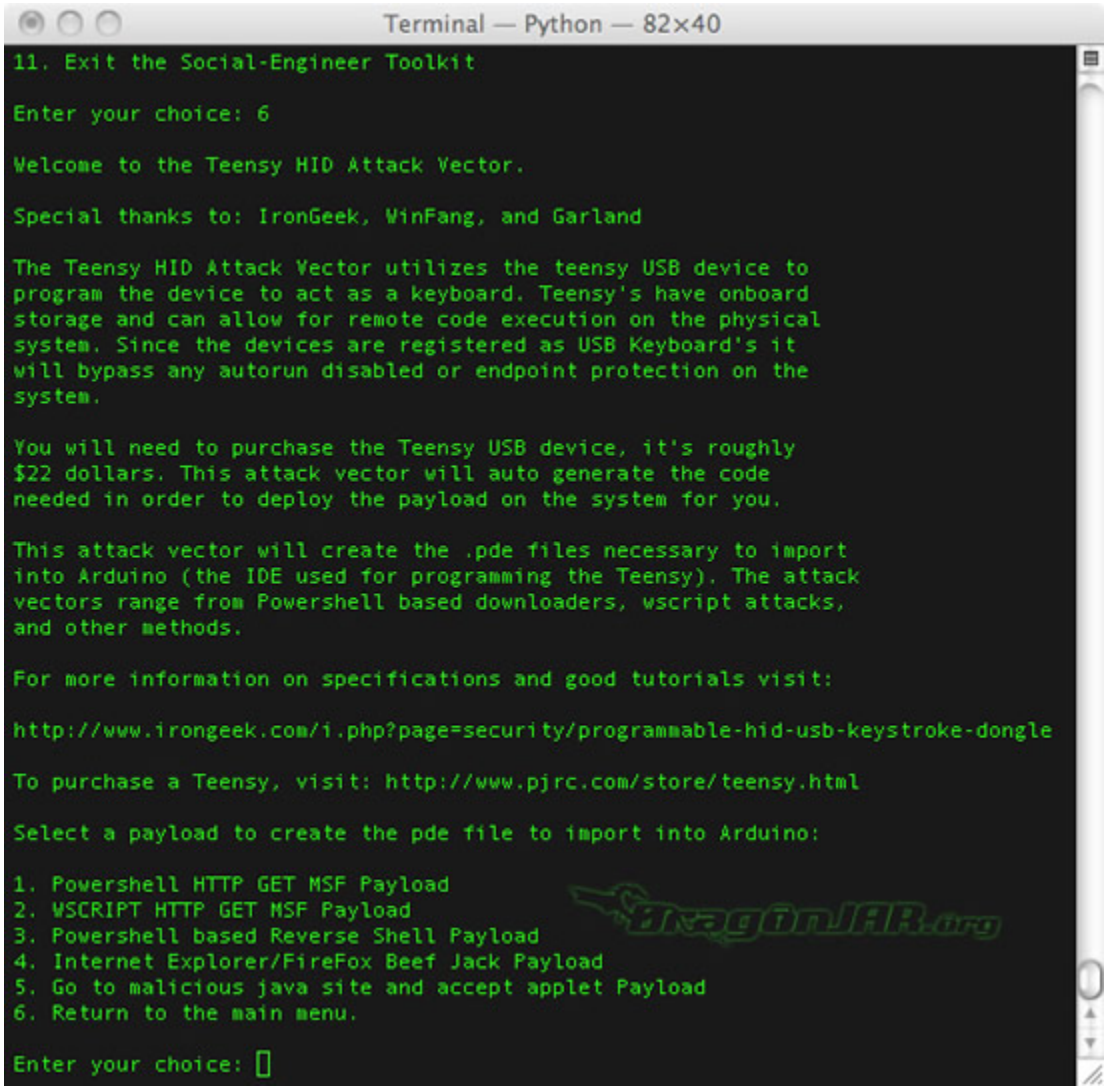
En esta completa suite para hacer ataques de ingeniería social, se incluye una sección especialmente dedicada al correo electrónico, permitiendo enviar correos falsos o desde una cuenta gmail, a una o muchas personas.



Ataques con dispositivos Personalizados en el The Social-Engineer Toolkit

Los dispositivos Teensy son todos aquellos aparatos en los que se ha utilizado la tabletaprogramable Teensy en su elaboración, al ser altamente personalizable y programable se puede emplear en procesos de auditorías en seguridad como ya nos ha mostrado IronGeek en la defcon 18 y SET nos facilita la tarea al

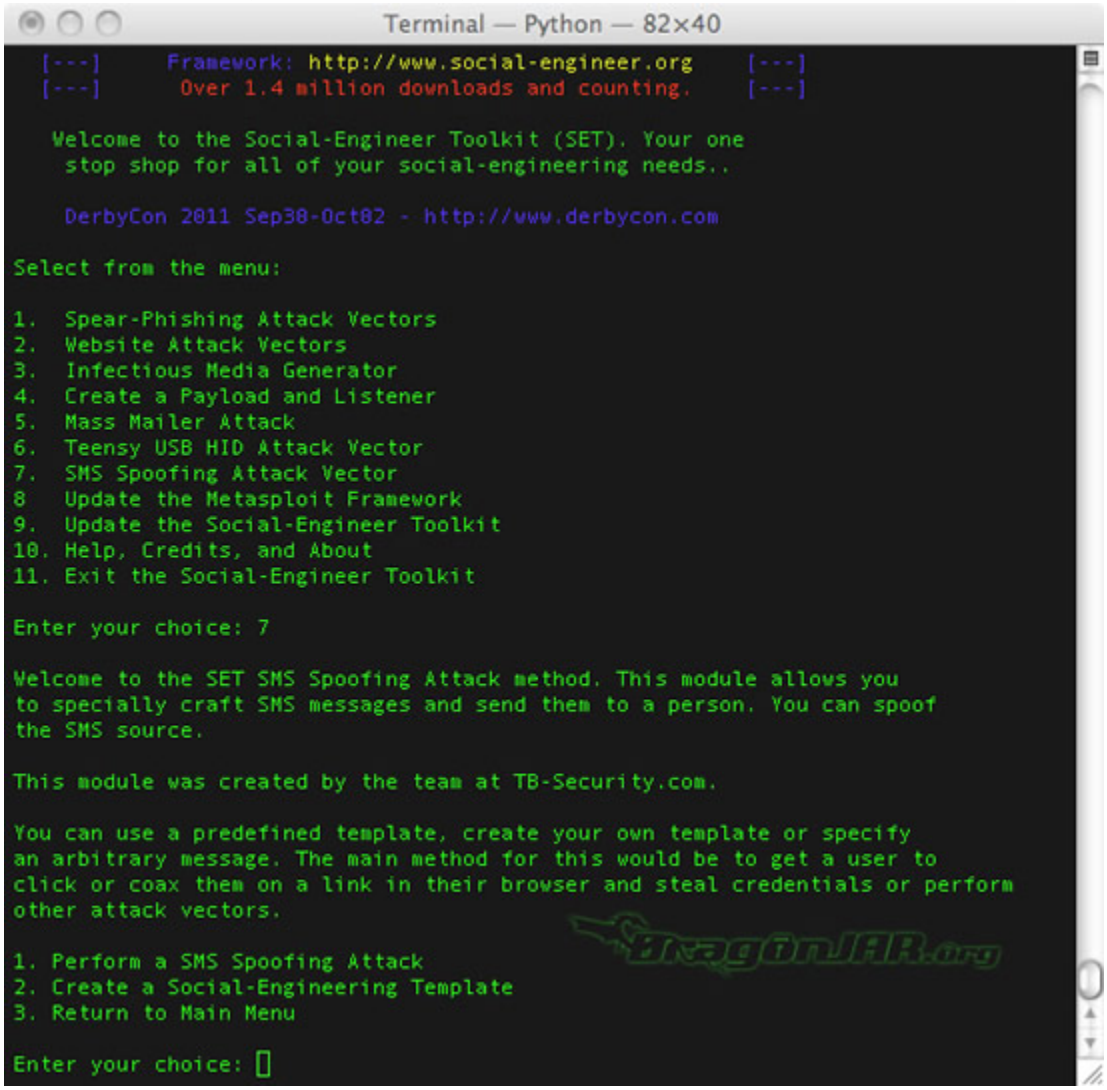
programar estos dispositivos, ofrecernos rutinas que al conectar un dispositivo de estos nos podría poner a bajar una aplicación externa o ingresar a un sitio especifico y aceptar un applet de java, infectándonos en el proceso.



Falsificando Mensajes de texto en el The Social-Engineer Toolkit

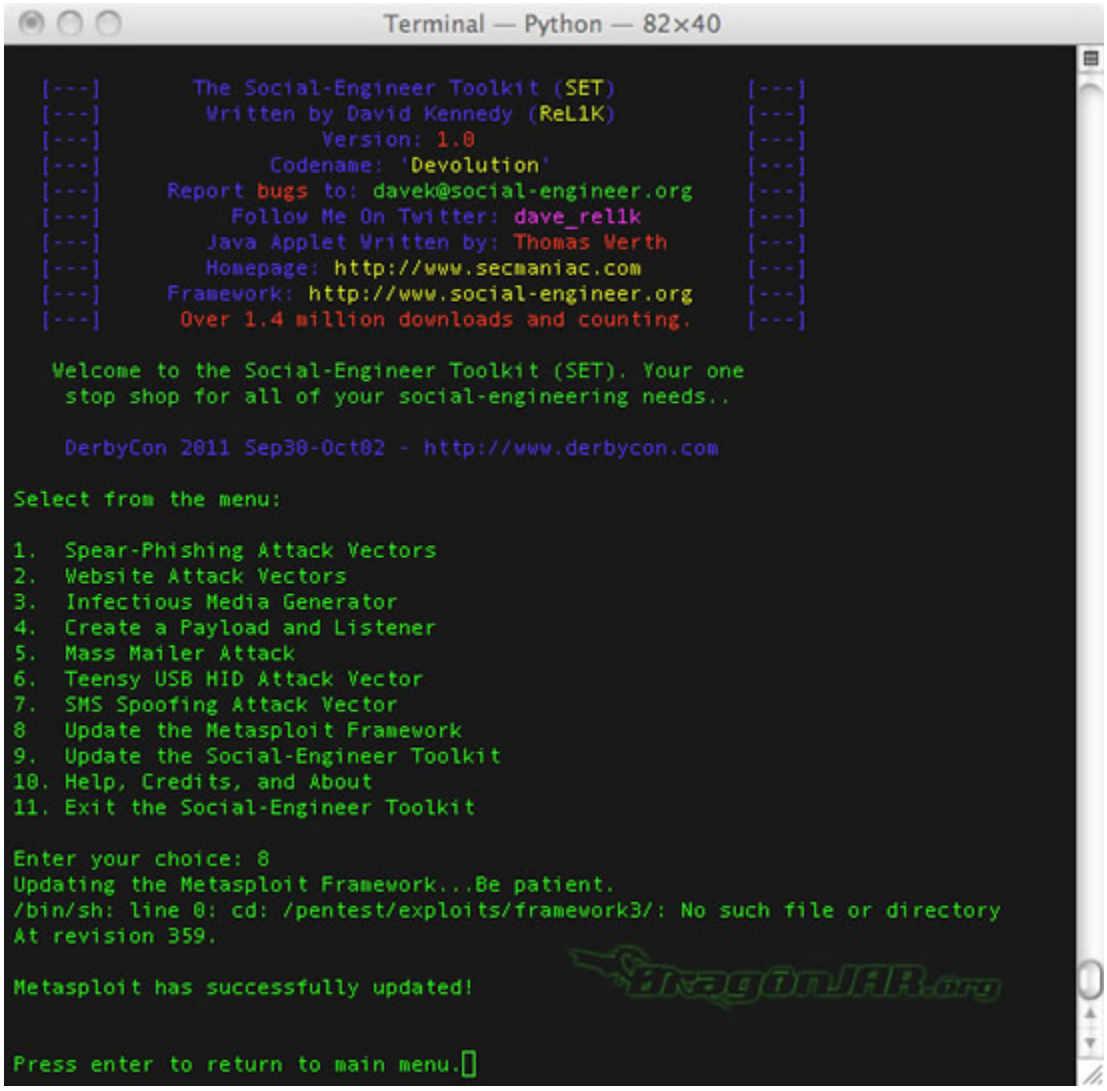
Uno de los vectores de ataques más eficientes a los que tenemos acceso con el SET, es el de envío de SMS (mensajes de textos) falsos, con los que podemos suplantar el número telefónico que envía el mensaje, haciéndole pensar al receptor que efectivamente esa persona es quien le ha escrito, también incluye una

opción para el envío masivo de SMS, por lo que podríamos enviar el mensaje a un mayor número de destinatarios sin problema (la posibilidad de envíos a teléfonos fuera de estados unidos, depende de la disponibilidad del servicio por parte de las empresas prestadoras SohoOS, Lleida.net, SMSGANG).



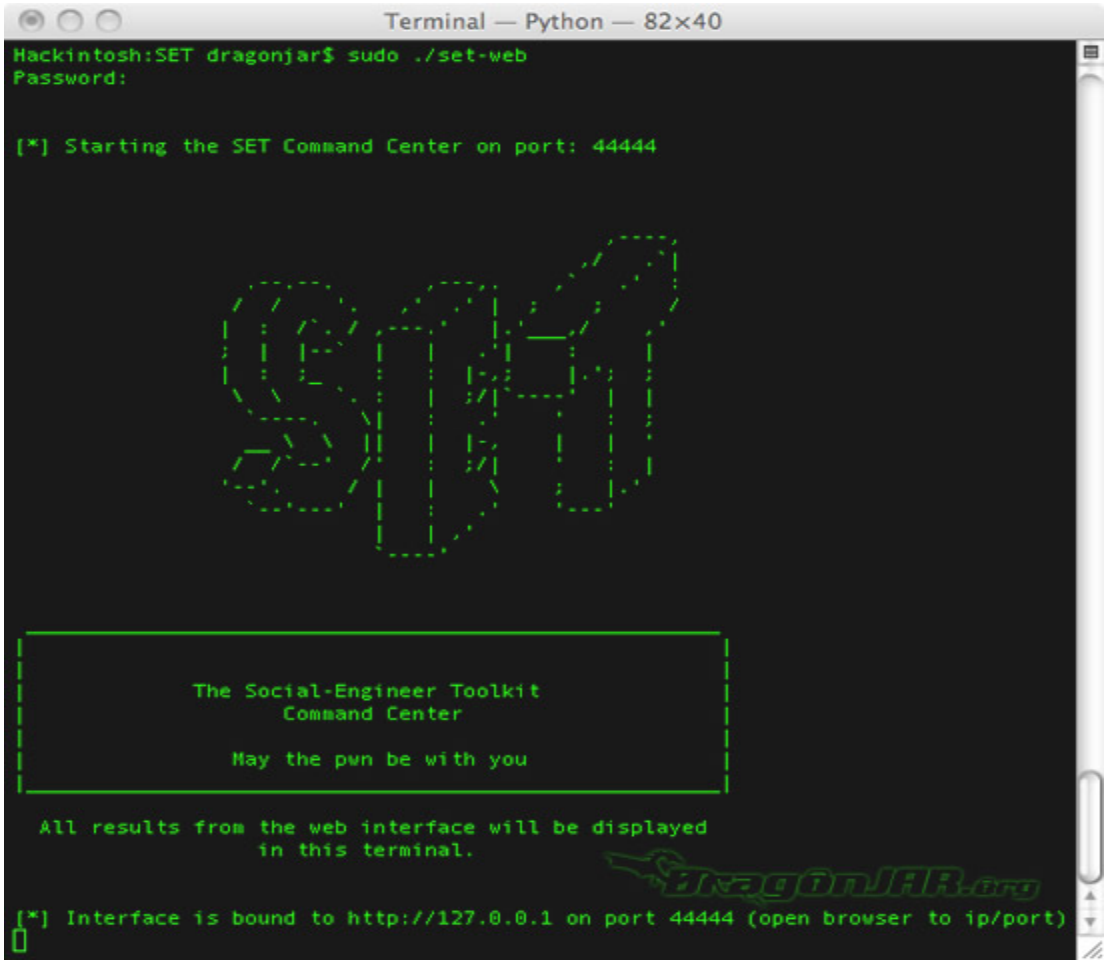
Actualizando Metasploit y The Social-Engineer Toolkit

El SET está ligado fuertemente al metasploit Framework, ya que muchas de sus funcionalidades las saca de este, por tanto incluye la posibilidad de actualizarlo desde su propia interface, así como incluye un actualizador para el mismo (recomendable que lo hagas cada que inicies el programa).



La interface web de The Social-Engineer Toolkit

En la versión 1.0 del SET se ha integrado una interface web, para lanzar todos los tipos de ataque que mencionamos anteriormente, para iniciar esta interface, solo tienes que ejecutar***./set-web*** o ***Python set-web***.



Abrimos la dirección **127.0.0.1:44444** en nuestro navegador y nos aparecerá la interface gráfica del SET, desde donde podremos lanzar cualquiera de sus ataques.

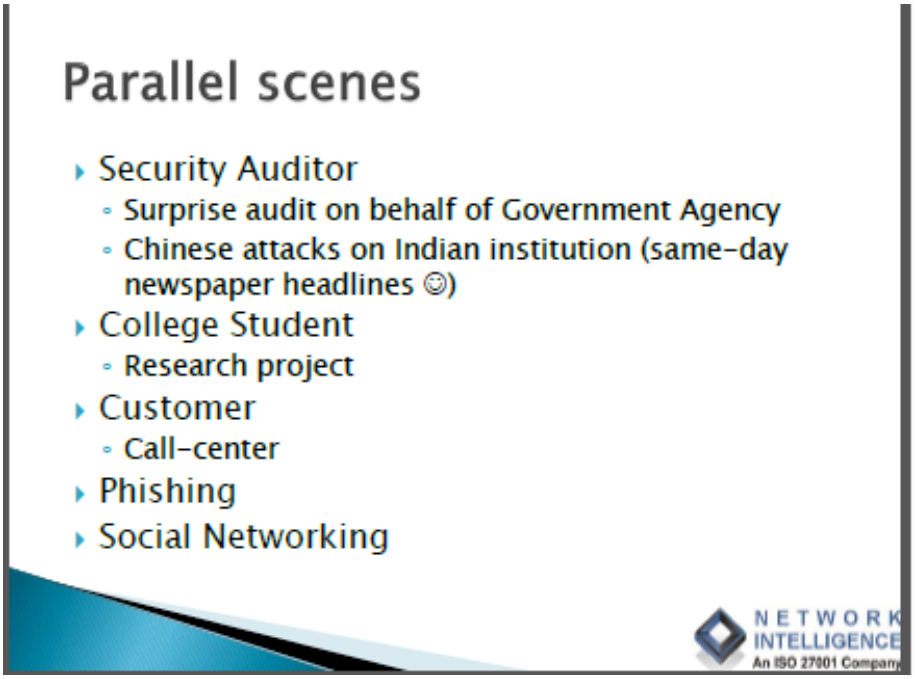
A continuación se deja la liga para que se observe el funcionamiento de la versión 1.0 del Social Engineer Toolkit: http://vimeo.com/16606897

Regresar a estudio realizado 2

ANEXO 3. INSTRUMENTO DE ESTUDIO REALIZADO 4

Preparación del escenario

Escenarios paralelos



Regresar a estudio realizado 4

ANEXO 4. RESULTADOS DEL ESTUDIO REALIZADO 6

Following table shows the result of above techniques. [6]

Case Study Result		
Case	**Number of target**	**Success**
1	5	80
One instance didn't work, as run at office in Underprivileged user mode and hence didn't work.		
2	3	100
Worked 100 percent as every one has executed it in root mode.		
3	2	50
One of the target users has not followed the Link provided in mail		

Regresar a estudio realizado 6