UNIVERSIDAD DON BOSCO

VICERRECTORIA DE ESTUDIOS DE POSTGRADO

TRABAJO DE GRADUACION

INGENIERIA SOCIAL, EL ELEMENTO HUMANO DE LA SEGURIDAD; CONTRAMEDIDAS Y PLANES DE ACCION PARA FORTALECER LA SEGURIDAD EN LAS ORGANIZACIONES.

PARA OPTAR AL GRADO DE

MAESTRO EN SEGURIDAD Y GESTION DE RIESGOS INFORMATICOS.

ASESOR

MG. JOSE GUTIERREZ

PRESENTADO POR:

LIC. MAURICIO E. CASTRO

Antiguo Cuscatlán, La Libertad, El Salvador, Centroamérica.

Enero 2016

Ingeniería Social, El Elemento Humano de la Seguridad. Contramedidas y Planes De Acción Para Fortalecer La Seguridad En Las Organizaciones.

Mauricio Castro,
mcastro@lageo.com.sv

***Resumen*—En el presente artículo se hace un estudio y análisis de las técnicas de ataque que hacen uso de la Ingeniería Social. Aun cuando la seguridad de la información cuenta con mucha tecnología para su protección, los sistemas siguen siendo vulnerables a los ingenieros sociales. Se presenta la metodología con la cual proceden los cibercriminales con el objetivo de vulnerar la seguridad de una empresa y así robar información sensible. Finalmente se muestran diferentes estrategias y medidas preventivas para combatir los ataques de Ingeniería Social, fortalecer la seguridad y elevar el nivel de defensa del eslabón más débil en la cadena de seguridad, el ser humano.**

***Términos Índices*—Amenaza, Dumpster Diving, Ingeniería Social, Ingeniería Social Inversa, Ingeniero social, Phising, Shoulder Surfing, Programa de Seguridad, Vulnerabilidad.**

I. Introducción

La Ingeniería Sociales la adquisición de información acerca de sistemas informáticos a través de medios que no involucran herramientas tecnológicas avanzadas. Esta técnica no requiere herramientas de punta, puede ser usada por personas con conocimientos técnicos moderados o bajos, y su uso es relativamente barato en el tema de costos [1]. Una organización puede adquirir toda la tecnología en seguridad que su presupuesto pueda costear, puede entrenar y capacitar a su personal en el uso de esta tecnología para resguardar la información sensible. El personal puede elaborar políticas de seguridad y seguir todas las buenas prácticas de los expertos. Puede también contratar guardias altamente entrenados para la seguridad física de las instalaciones. Sin embargo la empresa aun tiene una vulnerabilidad residual. La seguridad a menudo es simplemente una ilusión, una ilusión a menudo empeorada cuando la credulidad, la inocencia o la ignorancia entran en juego. Bruce Schneier, consultor de seguridad afirma que "La seguridad no es un producto, es un proceso" [2]. La seguridad no es un problema tecnológico, es un problema humano y de gestión.

El presente trabajo está organizado de la siguiente manera, primero se muestra la metodología que los ingenieros sociales usan para perpetuar un ataque junto con sus cuatro filosofías básicas [3], luego se describe las técnicas más comunes de Ingeniería Social en uso. Se realiza un estudio sobre la conciencia de la seguridad de la información en dos empresas salvadoreñas y se presenta su análisis. Finalmente se presentan las contramedidas, con el objetivo de elaborar una estrategia de prevención y el fortalecimiento de la seguridad de las organizaciones, de la información y de los usuarios. Los planes de acción van orientados a la elaboración de políticas y procedimientos, así como al entrenamiento de las personas en donde todos son parte fundamental en la cadena de la seguridad en la organización.

II. Estado del Arte

El termino Ingeniería Social es relativamente nuevo y sus orígenes se trazan a inicios del año 2000. Antes de esa coyuntura el término era poco conocido, sin mucha relevancia, y los estudios realizados eran mayormente en la lectura del lenguaje corporal, en el arte de descifrar las actitudes de un ladrón, sus gestos, el mensaje que proyectaba con su cuerpo. La difusión y uso del conocimiento en esta materia era poca, la información por la red era limitada, viajaba más lenta, y el interés por profundizar en esta área bastante escaza. Pocos autores encontramos que estudian los vínculos entre el arte del engaño y los ataques a los sistemas informáticos. La comprensión de las debilidades y riesgos inherentes en los seres humanos que crean y manipulan los sistemas no era primordial. En ese entonces las tecnologías estaban al alza, sin embargo, sistemas y tecnologías como las redes sociales y dispositivos móviles no tenían la inmensa difusión que tienen ahora en nuestra vida cotidiana. Esta primera ola de transformación digital trajo consigo la introducción de internet, pero 15 años después las cosas han cambiado. Una segunda ola ha traído la movilidad, las redes sociales son la principal manera, así como la favorita, de conectarse a la red y con las personas para compartir nuestra información, sea estos puntos de vista políticos, religiosos, personales, fotos familiares, ubicación personal, hacer mercadeo, etc.
Hay más dispositivos móviles que seres humanos en el planeta en este momento, se estima que hay más de 13,400 millones dispositivos conectados a internet, una cifra que equivale a más de dos veces el número de la población mundial y la tendencia es un incremente del 283% para el año 2020 [27]. Con el incremento de tecnología, potencia y capacidades en manos de millones de usuarios, los riesgos también han incrementado exponencialmente.

Actualmente el tema de la Ingeniería Social está siendo investigado con más profundidad cada día. Este trabajo se basa en las investigaciones más sobresalientes y de más peso que hasta este momento se han realizado. La primera investigación es por Kevin Mitnik, famoso consultor estadounidense y experto en seguridad informática, primeramente conocido como un hacker y por sus problemas con la ley, pero luego como un consultor de seguridad que utilizo su conocimiento y habilidades para entrenar y enseñar a organizaciones y gobiernos en el tema de la seguridad de la

información. El libro titulado <El Arte del Engaño> de Kevin Mitnik es quizá el más citado en todas las investigaciones posteriores realizadas sobre el tema de la Ingeniería Social. Aun cuando este trabajo se realizó en el 2002 sus aportes tiene una gran vigencia ya que la tecnología cambia rápidamente, pero los patrones humanos, sus vulnerabilidades y su manera (ilógica muchas veces) de actuar se mantienen. Innumerables trabajos se han fundamentado en esta investigación, agregándole el ingrediente particular y la orientación deseada según la época y las necesidades propias. Por eso se ha considerado muy importante incluir este material como referencia en esta investigación.

Un segundo estudio realizado en el área de Ingeniería Social es la tesis doctoral del Dr. Marcus Nohlberg, PhD en ciencias de la computación en la universidad de Skövde, Suecia en 2007. Marcus Nohlberg, autor de la figura 1, diferenció en su tesis doctoral hasta seis disciplinas diferentes: sociología, psicología, economía y gestión, seguridad, derecho y educación. En este trabajo se tratan las aéreas de psicología, gestión del riesgo y la seguridad y educación del usuario. Esta tesis, una de las más completas y consultadas también se basó primordialmente en los trabajos de Kevin Mitnik en su libro El Arte del Engaño.

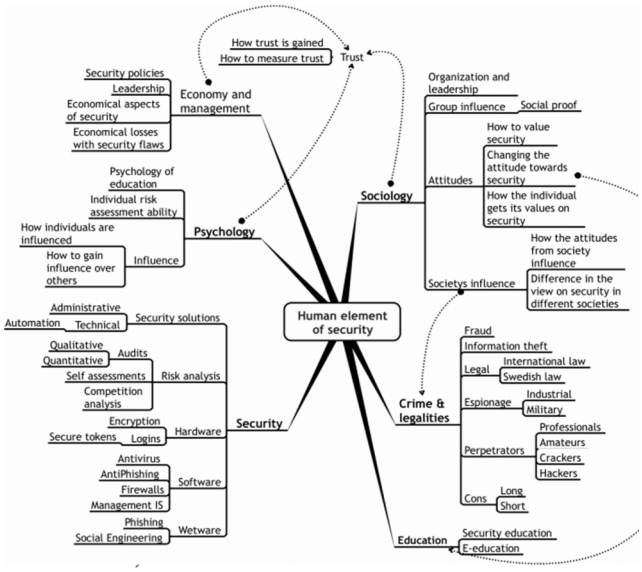


Fig. 1. Aéreas de investigación y tópicos conectados al elemento humano de la seguridad en la I.S. [28]

Ingeniería Social Automatizada

La Ingeniería Social Automatizada es una evolución de la Ingeniería Social, basada en la automatización de los componentes presentes. Estos componentes suelen ser el medio y el atacante. Además, conlleva un cambio de filosofía a la hora de diseñar el pretexto. La diferencia entre una herramienta que automatiza la faena y una prueba de concepto de la Ingeniería Social Automatizada es la independencia que esta segunda toma a la hora de realizar el ataque, gracias a la presencia de elementos psico-sociales incorporados a su lógica de control. El concepto está muy enlazado con la inteligencia artificial, dada la necesidad de mutar con nueva información y actualmente se han llevado pruebas de concepto y estudios en este campo. En la figura 2 se muestra un esquema genérico del ciclo de ataque, y procesos se ejecutan dentro de un bot en la Ingeniería Social Automatizada.

Como principales autores de este nuevo concepto están Markus Huber con su tesis de máster en Computer Science [29] y el equipo francés EURECOM con su trabajo titulado "HoneyBot" [30]. Ambos estudios desarrollaron software tipo bots para mantener conversaciones e interacciones automatizadas en Facebook, con altos índices de respuesta y muy bajos porcentaje de detección.

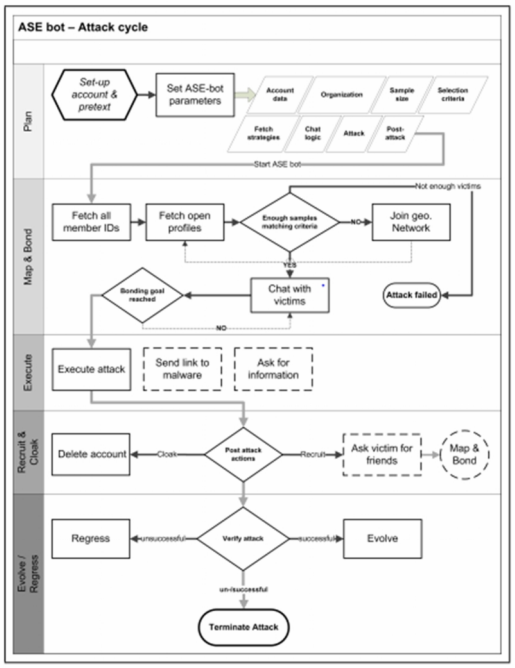


Fig. 2. Muestra el ciclo de ataque del un bot en la I.S.A

III. DESCRIPCIÓN DE LA PROBLEMÁTICA

Los controles técnicos estrictos parecen no ser una solución viable a los problemas asociados con los seres humanos y la seguridad. De hecho, muchos usuarios saben que su comportamiento no es compatible con las políticas de seguridad actuales en lasorganizaciones y en su lugar encuentran justificaciones en el comportamiento similar de sus compañeros de trabajo, piensan "todos lo hacen", y en la creencia de que los reglamentos internos de la organización no son realistas.En un estudio llevado a cabo por inspectores del Departamento del Tesoro de los Estados Unidos, un tercio de los empleados del Servicio de Impuestos Internos (IRS) divulgó sus nombres de usuario y contraseñas a los auditores que llamaron fingiendo ser técnicos de soporte [31].

La problemática podemos resumirla en la siguiente frase: "No importa toda la tecnología que se tenga - no hay tecnología que pueda proteger contra los seres humanos". La firma de seguridad Gartner Inc. expreso lo siguiente referente al problema de los riesgos involucrados con los seres humanos: "Los individuos malintencionados siempre han

sabido que la mejor manera de burlar cualquier sistema de seguridad es manipular un objetivo humano dándoles lo que quieren - lo que llamamos Ingeniería Social. Esto sigue siendo la mayor amenaza de seguridad a las empresas" [28].

Es evidente que hay grandes riesgos asociados con los seres humanos y la seguridad, y sobre todo en lo que respecta a los ataques dirigidos a las vulnerabilidades humanas. En el mundo de la seguridad de la información, se sabe relativamente poco sobre qué es lo que hace que un ataque de Ingeniería Social tenga éxito, como se puede medir, y lo más importante que es cómo prevenirlo. Si no se conoce la envergadura del riesgo, no se puede juzgar con objetividad si una política o medida aumenta realmente la seguridad o si solo es un mero formalismo. Si queremos proteger un sistema debemos saber y comprender contra que debemos protegerlo. De esta manera, si se ignoran los ataques realizados hacia los seres humanos, se está asegurando que contra estos ataques se está totalmente vulnerable. La seguridad de la información se debe abordar de una manera holística. Este trabajo se enfoca en el elemento humano de la seguridad, abordando la técnica de ataque llamada Ingeniería Social.

IV. METODOLOGÍAS DE LA INGENIERÍA SOCIAL

Existe un patrón común que un ingeniero social sigue para llevar a cabo un ataque. Según un estudio llevado a cabo por la empresa consultora Gartner, todo cibercriminal sigue una serie de pasos comunes que son reconocibles y prevenibles [4]. Este patrón común es una metodología de cuatro fases: 1-recopilar información, 2-desarrollar una relación, 3-ejecución y 4-explotación [4]. En la figura 3 vemos el esquema del patrón de ataque según Kevin Mitnik

A. *Recopilar Información.*

En esta fase el atacante puede usar un sin número de técnicas para recopilar información de su víctima o de alguna persona clave en la ejecución del ataque. Alguna información útil incluye, pero no está limitada a: lista de teléfonos, lista de contactos, lista de correos electrónicos, fechas de cumpleaños, el organigrama de alguna organización.

B. *Desarrollar una relación de confianza con la víctima.*

El atacante busca explotar la vulnerabilidad psicológica de la buena disposición o la "buena voluntad" de las personas para mantener y desarrollar una buena relación con las víctimas. Cuando el ingeniero social logra situarse en una posición de "confianza" luego puede usarla para explotar esta vulnerabilidad.

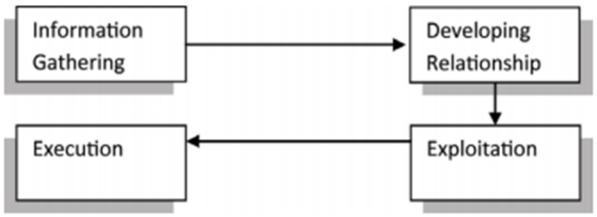


Fig. 3. Muestra del patrón de ataque de cuatro pasos dela Ingeniería Social

C. *Ejecución.*

El objetivo ahora puede ser manipulado por el agresor "de confianza" para revelar la información (por ejemplo, contraseñas) o realizar una acción (por ejemplo, crear una cuenta) que normalmente no ocurriría. Esta acción podría ser el final del ataque o el comienzo de la siguiente etapa.

D. *Explotación.*

Una vez que la víctima ha completado la tarea solicitada por el ingeniero social, el ciclo ha sido completado.

V. MOTIVACIONES DEL LOS ATAQUES DE INGENIERÍA SOCIAL.

Según un estudio patrocinado por la empresa de seguridad CheckPoint la principal motivación de los ataques de Ingeniería Social es la obtención de un beneficio económico [5]. Motivaciones para ataques de Ingeniería Social varían ligeramente en los diferentes países.

A. Motivaciones económicas: existe una variedad de razones por las que alguien justifique un ataque para obtener ganancias económicas. Sin embargo todas son ilegales e infringen la ley. Un ejemplo típico de esta motivación es el robo de tipo hormiga que se hace a los bancos [12].

B. Intereses propios: un individuo puede, por ejemplo, querer acceder y/o modificar la información que se asocia a un familiar, amigo o incluso un vecino. Por ejemplo modificar el balance de la tarjeta de crédito o borrar el historial de esquelas.

C. Venganza: por razones muy particulares y específicas de una persona, esta puede elegir una víctima como un amigo, un vecino, un compañero de trabajo o una organización, con el simple propósito de satisfacer la necesidad emocional de la venganza.

D. *Presiones Externas:* una persona puede estar recibiendo la presión de los amigos, la familia ogrupos del crimen organizado por razones tales como el beneficio económico, el interés personal, interés político y/o espionaje industrial.En los últimos años se conocieron tres incidentes a gran escala: Stuxnet, Duqu y Flame –poderosos códigos maliciosos dirigidos contra plantas industriales ubicadas en Oriente Medio y Europa– cuyos objetivos apuntaron al saboteo y al robo de información [13].

La tendencia muestra que los atacantes continuarán utilizando Ingeniería Social para obtener información valiosa de los demás. Estos utilizan cuatro filosofías:

1. Actúan con fianza y llaman la atención en lugar de esconderse y parecer sospechoso [7].Dan algo a la víctima, para generar reciprocidad y confianza [8].
2. Usan el humor como herramienta para que las personas no estén a la defensiva [9].
3. Solicitan y luego proporcionan unas respuestas que suenan legítimas [10]

7 de cada 10 personas caen ante un esquema similar al expuesto [11].

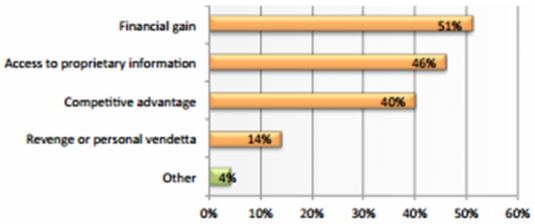


Fig. 4. Principales motivaciones para los ataques de Ingeniería Social. [14]. El cuadro muestra que la principal razón sigue siendo el lucro económico.

VI. VULNERABILIDADES PSICOLÓGICAS EXPLOTADAS POR EL INGENIERO SOCIAL.

La manipulación ha sido estudiada por los científicos sociales durante al menos cincuenta años. En este trabajo se estudió en las investigaciones del científico social Robert B. Cialdini, en su libro <YES, 50 Maneras Probadas para ser Persuasivo>, en el cual se evidencian seis "tendencias básicas de la naturaleza humana" que están involucrados en un intento de manipular y obtener con éxito la acción deseada ante una solicitud hecha por un ingeniero social.

Estas seis tendencias son en las que los ingenieros sociales se basan (consciente o inconscientemente) en sus intentos de manipular a sus víctimas para robar información y penetrar en los sistemas de seguridad que a ellos les interesa.

A. *Autoridad.*

La gente tiene una tendencia a cumplir cuando una solicitud es hecha por una persona con autoridad. Una persona puede estar convencido de cumplir con una solicitud si él o ella cree que el solicitante es una persona con autoridad dentro de la organización o una persona que esté autorizado para hacer tal petición.

Un ejemplo de ataque explotando esta vulnerabilidad se da cuando un ingeniero social intenta encubrirse a sí mismo bajo el manto de la autoridad al afirmar que él es parte del departamento de TI, o que es un ejecutivo o trabaja para un ejecutivo de la empresa.

B. Simpatía.

La gente tiene la tendencia a cumplir con las solicitudes cuando la persona que ha solicitado ha sido capaz de establecerse como simpático, o que tienen intereses similares, creencias y actitudes como las de su víctima.

Ejemplos de ataques usando la simpatía es cuandoa través de la conversación, el atacante logra inferir una afición o interés de la víctima, y alega un interés y entusiasmo por la misma afición. También el atacante puede presumir ser del mismo pueblo o la escuela, o tener metas similares. El ingeniero social también intentará imitar los comportamientos de su objetivo para crear la apariencia de similitud.

C. *Reciprocidad.*

Podemos cumplir automáticamente con una solicitud, cuando se nos ha dado o prometido algo de valor con anterioridad. El regalo puede ser un elemento de material, o consejo, o ayuda. Cuando alguien ha hecho algo para usted, se siente una inclinación a corresponder automáticamente debido a esta vulnerabilidad psicológica. Esta fuerte tendencia a corresponder existe incluso en situaciones en que la persona recibe un regalo que no ha pedido. Una de las maneras más eficaces para influir en la gente para que nos haga un "favor" (que cumpla con una solicitud) es dando algún regalo o ayuda que establece una línea de obligación o reciprocidad subyacente.

Los miembros de una secta religiosa Hare Krishna eran muy eficaces para influir en la gente mediante el principio de la reciprocidad. Para influenciar a que la gente diera donaciones para su causa, estos daban un libro o una flor como regalo. Si el receptor trataba de devolver el regalo, el dador se negaba diciendo: "Es nuestro regalo para ti". Este principio de comportamiento de la reciprocidad fue utilizado por la secta para aumentar sustancialmente las donaciones [23].

Un claro ejemplos de un ataque usando la reciprocidad es: un empleado recibe una llamada de una persona que se identifica a sí mismo como del departamento de TI. La persona que llama, explica que algunas computadoras de la compañía han sido infectadas con un virus nuevo no reconocido por el software antivirus que puede destruir todos los archivos en un ordenador, y se ofrece a indicar la persona (victima) a una serie de pasos para evitarproblemas. Después de esto, la persona que llama pide a la víctima que pruebe una nueva utilidad de software que acaba de ser actualizado recientemente para permitir a los usuarios cambiar las contraseñas. El empleado que recibe la llamada, es decir la víctima, es reacio a rechazar la ayuda, porque la persona que llama, el ingeniero social, ha proporcionado ayuda que supuestamente protege al usuario de un virus. Él empleado en este caso es reciproco cediendo a la petición de lapersona que llama, exponiendo la seguridad de la organización.

D. Consistencia.

La gente tiene la tendencia a realizar una acción después de haber hecho un compromiso público o después de haber avalado algo por una causa. Una vez que hemos prometido públicamente que vamos a hacer algo, no queremos parecer poco fiables o indeseables y tenderemos a seguir adelante con el fin de ser coherentes con nuestra declaración o promesa.

El siguiente es un ejemplo de un ataque a esta vulnerabilidad: El atacante contacta a un empleado nuevo relativamente y le asesora de recordar cumplir con ciertas políticas y procedimientos de seguridad como condición para que se le permita utilizar los sistemas de información de la compañía. Después de discutir algunas prácticas de seguridad, la persona que llama pide al usuario su contraseña "para verificar el cumplimiento" con la política en la elección de una contraseña difícil de adivinar. Una vez que el usuario revela su

contraseña, la persona que llama hace una recomendación para construir contraseñas futuras de tal manera que el atacante será capaz de adivinar. La víctima cumple en este caso debido a su acuerdo previo de cumplir con las políticas de la compañía y bajo el supuesto de que la persona que llama no está más que verificando su cumplimiento.

E. Validación Social.

La gente tiene la tendencia a hacer cosas que otros parecen estar haciendo. La acción de los demás es aceptada como la validación de que el comportamiento en cuestión es la acción correcta y apropiada. El Dr. Cialdini en su libro <YES, 50 Maneras Probadas para ser Persuasivo> dice que hay un efecto del tipo "magnetic middle" en el cual las personas siguen las actitudes que el promedio de las personas en general siguen. Es una tendencia natural del ser humano a hacer lo que la mayoría de personas están haciendo, aun cuando su acción no desea deseable. En este sentido, las personas tratan de estar alineados con la norma del comportamiento medio, es decir buscando una validación social [24.]

Para ejemplificar un ataque de este tipo daremos el siguiente ejemplo: una persona llama y dice que está llevando a cabo una encuesta y brinda algunos nombres de otras personas en el departamento sobre los cuales dice ya han cooperado con él en la encuesta. La víctima, creyendo que la cooperación de los demás valida la autenticidad de la solicitud, se compromete a participar. La persona que llama y luego hace una serie de preguntas, entre las que se encuentran preguntas disfrazadas con el objetivo de seducir y engañar a la víctima para que revele su nombre de usuario y contraseña de equipo. De hecho, se han realizado experimentos en donde, mediante "encuestas" las personas entregan información sensible de la organización exponiendo su seguridad, y un ejemplo de ello fue la realizada por Info Security Europe, en donde 155 empleados fueron entrevistados para probarlo. La encuesta fue realizada por los organizadores de una feria de seguridad de la información en una búsqueda para averiguar que tanto los trabajadores tienen conciencia de la seguridad y de la importancia de la información de la empresa almacenada en sus computadoras [25].

F. Escasez.

Las personas tienen la tendencia a realizar una acción o cumplir con una solicitud cuando creen que el objeto buscado es escaso y otros están compitiendo por él, o que sólo está disponible para un corto periodo de tiempo. El Concepto de escasez como herramienta de persuasión se basa en el hecho que las oportunidades nos parecen más valiosas cuando su disponibilidad es limitada**.** La idea de una pérdida potencial juega un papel muy importante en nuestra toma de decisiones. De hecho la gente parece más motivada por la idea de perder algo que por la idea de ganar algo (aversión al riesgo). A medida que las oportunidades se vuelven menos disponibles, perdemos libertades. Y el ser humano odia perder las libertades que tiene [26].

Ejemplo de ataque: Un atacante envía mensajes de correo electrónico afirmando que las primeras 500 personas que se registren en el "nuevo sitio web" de la empresa van a ganar entradas gratis para alguna película de estreno. Un empleado desprevenido se registra en el sitio, y se le pide que proporcione su dirección de correo electrónico de la empresa y que elija una contraseña. Muchas personas, motivadas por la conveniencia, tienen la tendencia a utilizar la misma contraseña o una similar sobre cada sistema informático que utilizan, sea esta su cuenta personal de correo, su clave para ingresar a su computadora en la empresa, o su clave para su cuenta de banco. Aprovechándose de esto, el atacante intenta comprometer los sistemas del trabajo de la víctima y equipos domésticos con el nombre de usuario y contraseña que se han introducido durante el proceso de registro en el sitio Web.

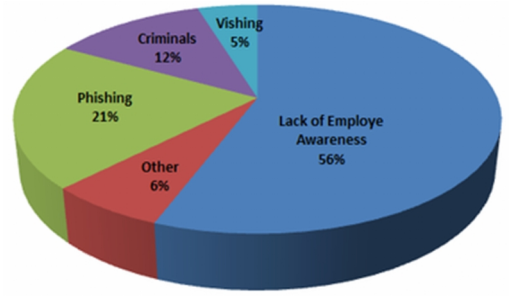


Fig. 5. Amenazas más dañinas para una organización. El cuadro muestra la importancia del Gobierno de Seguridad de TI en el tema de Ingeniería Social [15].

VII. TÉCNICAS DE ATAQUE DE LA INGENIERÍA SOCIAL

Las técnicas empleadas durante un ataque de Ingeniería Social en gran medida dependen de la fuerza, destreza y habilidad de la persona que los ejecuta. Aquí mencionamos las técnicas más usadas, como se muestra en la figura 6, las cuales no involucran grandes conocimientos técnicos ni costos económicos, esto las convierte muy atractivas y para practicar aun cuando el atacante sea novato y no cuente con mucha expertise [6].

A. Shoulder Surfing.

Esta técnica consiste en obtener información de una pantalla por estar físicamente cerca de ella y tener acceso a la lectura de la información digitada en la pantalla. La forma más habitual en que esta técnica es puesta en práctica es durante el uso de los cajeros automáticos o bien cuando un usuario despistado digital su contraseña sin cuidado de las personas alrededor. Por ética y buena costumbre las personas deben observar en otra dirección cuando alguien cercano está ingresando sus credenciales personales en su teléfono, tablet, laptop o computadora.

* *Contramedidas:* esté siempre consiente de las personas a su alrededor y que es lo que hacen. Los lugares más comunes para estas prácticas son las filas en los cajeros automáticos, en la oficina al ingresar las credenciales en los sistemas y lugares públicos al momento de hacer uso de teléfonos inteligentes. Siempre hay que estar prevenido al momento de realizar transacciones en aeropuertos, estaciones de tren, restaurantes, cafés y cualquier área pública.

Se recomienda no realizar transacciones que involucre información sensible de la organización si no se está libre del riesgo de sufrir shoulder surfing. También es recomendable solicitar una pantalla protectora de privacidad para la computador móvil asignada por la empresa.

B. Dumpster Diving.

Es el acto de colectar y realizar un análisis de los documentos y otros materiales que son desechados en los cestos de basura de una organización para encontrar información sensible. Con esta información el atacante se documenta de la manera de trabajar en la compañía, de su manera de proceder y de datos importantes por lo tanto tendrá más éxito al momento de perpetuar un engaño. Cuando una persona suele tener mucho conocimiento de una compañía, es muy probable que el personal de esta asuma que es un empleado legítimo, desconfiando menos para entregar información o realizar una acción solicitada por el atacante. Información aparentemente sencilla como, listas de números de teléfonos, calendarios, estados de tarjetas de crédito, recibos o estructura organizativa, pueden facilitarle el ataque a un ingeniero social. Esta información se complementa con la información que las personas voluntariamente comparten en las redes sociales, ya sea personal o corporativa.

**Contramedidas:* Las buenas prácticas de seguridad dictan tener una política para la destrucción del material físico y digital. De esta manera toda la papelería con información sensible debe ser destruida en un triturador de papel. En el ámbito digital, todo dispositivo que contenga (o haya contenido) información sensible corporativa debe seguir el procedimiento llamado "whipping" para evitar que posteriormente alguien intente hacer una restauración de información contenida en el. Con este procedimiento se garantiza un borrador definitivo de información actual y antigua. Más adelante en la sección de políticas de seguridad se habla más al respecto.

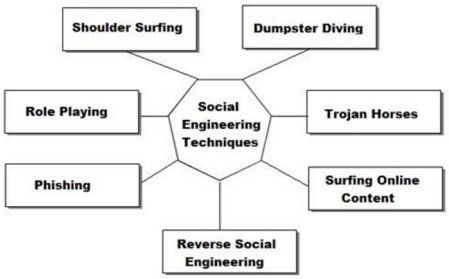


Fig. 6. Mapa mental de las técnicas más comunes de ataques de la Ingeniería Social

C. Phishing.

Se refiere al hacerse pasar por una entidad de confianza, es decir usurpar su identidad y hacer uso de esta confianza para adquirir información o manipular a alguien para ejecutar una acción. Una práctica común es construir una página web falsa idéntica a la de una institución bancaria por ejemplo, con el propósito de capturar credenciales de los usuarios. Este tipo de ataque generalmente se ejecuta mediante el envío masivo de correos electrónicos para "pescar" el mayor número de víctimas posibles y atraerlas al sitio web fraudulento. En ocasiones, el simple hecho de accesar a un sitio web elaborado por el atacante, compromete la seguridad del equipo y la red desde donde ha ingresado la víctima.

**Contramedidas:* Se recomienda verificar cuidadosamente cualquier correo electrónico sospechoso solicitando información. Hay que revisar todos los vínculos embebidos en el mensaje y nunca (nunca) enviar información personal. Al momento de recibir un correo solicitando confirmar alguna cuenta de usuarios o credenciales, es necesario llamar a la institución en cuestión informando de lo sucedido. Ninguna institución financiera o bancaria, por práctica general, solicita información personal por medio de correo electrónico. Ante cualquier duda en correos electrónicos recibidos siempre llamar al personal de TI de la organización.

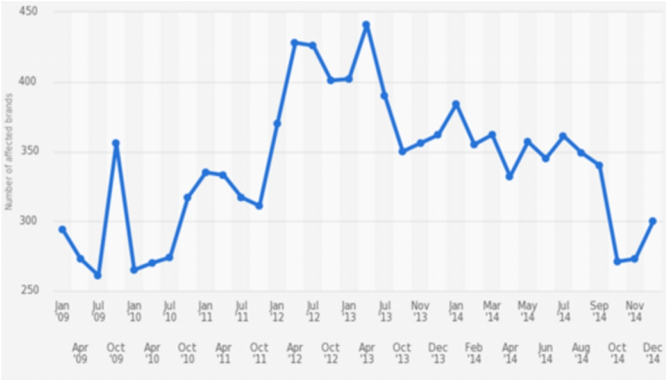


Fig. 7. Número de entidades legitimas que han sido blanco de ataques de phishing, en el periodo de 2009 – 2014 [32].

D. El usuario "importante".

Al fingir ser una persona importante de la organización con una necesidad urgente un Ingeniero Social puede ejercer presión para que el personal de TI revele información sensible, por ejemplo: el tipo de software usado para sesiones remotas, pasos para configurarlo, IP de conexiones y credenciales para el acceso. El usuario "importante "siempre apela al miedo o las consecuencias que podría tener el empleado, es decir la víctima, sino acata o colabora con la solicitud hecha de información o acción.

**Contramedidas:* Para contrarrestar este tipo de ataque la organización debe tener muy claras y difundidas sus políticas de revelación de información. De esta manera los empleados pueden actuar de manera segura, sin miedo a futuras consecuencias contra sus trabajos. Si un empleado tiene claro el tipo de información que está autorizado a revelar y a quienes, tendrá menos probabilidades de ser intimidado por algún usuario "importante". Es necesario el apoyo total de la alta dirección, pues se necesita su respaldo para proceder acorde con las políticas establecidas y para que incluso, un verdadero usuario importante, siga los canales oficiales y respete las políticas y procedimientos para la solicitud de información.

E. Ingeniería Social Inversa.

Consiste en crear un problema para una víctima y ofrecer ayuda a la víctima para resolver el mismo problema. De esta manera el atacante establece la confianza entre las partes, que se utiliza luego para explotar a la víctima para obtener la información sensible que el ingeniero social tiene como objetivo.

**Contramedidas:* para este tipo de ataques es fundamental tener siempre presentes las buenas prácticas de seguridad fundamentales de no revelar información sensible a personas no autorizadas. Si un empleado es completamente consiente de las políticas de seguridad, siempre estará atengo ante cualquier solicitud maliciosa de información. Aquí juega un papel fundamental el entrenamiento y concientización en temas de seguridad a los usuarios, lo cual abordaremos más adelante.

F. Baiting.

Es la táctica de dejar un medio de almacenamiento (por ejemplo, una memoria USB) dentro de una organización con un malware dentro del dispositivo (por ejemplo, un troyano o keylogger). El software malicioso se ejecuta automáticamente cuando se inserta en un ordenador. Generalmente en este tipo de ataque se explota la vulnerabilidad psicológica humana de la curiosidad [6]. Este tipo de ataque es en muchos aspectos similar a los ataques de phishing. Sin embargo, lo que los distingue de otros tipos de técnicas es la promesa de un artículo o bien que los hackers utilizan para atraer a las víctimas. Existe un ataque de prueba documentado de este tipo, en donde Steve Stasiukonis infecto docenas de memorias USB y las disperso en el paqueo de una organización. Muchos de los empleados insertaron estas USB en sus computadoras y así el atacante tuvo acceso a los sistemas [33].

**Contramedidas:* Para combatir este tipo de ataques será necesario tener usuarios informados en temas de seguridad y comprometidos a seguir los buenos hábitos y prácticas para garantizar la seguridad de la organización. Un programa detallado de entrenamiento sobre la seguridad de la información será siempre la mejor contramedida para evitar este tipo de ataques.

G. Generar una situación de hostilidad.

El humano tiende a cuestionar menos cuando una persona que está enojada. Los ingenieros sociales suelen fingir, por ejemplo, estar en una conversación telefónica acalorada para minimizar la probabilidad de ser cuestionados al momento de pasar por algún punto de seguridad física.

**Contramedidas:* Para combatir este tipo de ataques será necesario tener usuarios informados en temas de seguridad y comprometidos a seguir los buenos hábitos y prácticas para garantizar la seguridad de la organización. Un programa detallado de entrenamiento sobre la seguridad de la información será siempre la mejor contramedida para evitar este tipo de ataques.

H. Lenguaje corporal.

Con esta técnica el ingeniero social comunica sus falsas intenciones no solo verbalmente sino con su cuerpo. Una de las habilidades para desenmascarar a los ingenieros sociales es desarrollar la habilidad de leer el lenguaje corporal para diferenciar el natural del sospechoso, el congruente del incongruente con el mensaje verbal que se está recibiendo.

**Contramedidas:* la lectura del lenguaje del cuerpo es algo que se alcanza con los anos y después de mucha practica y observación, sin embargo para combatir este tipo de ataques será necesario tener usuarios informados en temas de seguridad y comprometidos a seguir los buenos hábitos y prácticas para garantizar la seguridad de la organización. Un programa detallado de entrenamiento sobre la seguridad de la información será siempre la mejor contramedida para evitar este tipo de ataques.

I. *Piggybacks Rides oTailgating.*

Esta técnica consiste en situarse cerca de una puerta de acceso a un edificio o campus y fingir ser un empleado legítimo. El ingeniero social aprovecha la oportunidad de que un empleado abra la puerta para seguirlo y así sobrepasar las medidas de seguridad. Una práctica común es presentarse en un día lluvioso con una caja pesada a la par de la puerta de acceso, para solicitar a un empleado, aprovechándose de la buena voluntad de las personas diciendo: ¿me abrirías la puerta por favor? No puedo alcanzar mi tarjeta de acceso en este momento. La mayoría de las personas caen en esta trampa.Pero esto también este ataque podría tomar la forma de alguien pidiendo prestado un teléfono o computadora portátil para llevar a cabo una acción simple cuando en realidad están instalando algún tipo de software malicioso.

**Contramedidas:* Deber ser un hábito de todos los empleados solicitar la identificación “aun en días lluviosos”. Si la persona olvido su carnet, existen otros medios para verificar la identidad de la persona y sus privilegios de acceso, estos pueden ser llamar consultando a su área o gerencia, a su jefe inmediato al departamento de RRHH, ante cualquier duda siempre será necesario consultar. Para combatir este tipo de ataques será necesario tener usuarios informados en temas de seguridad y comprometidos a seguir los buenos hábitos y prácticas para garantizar la seguridad de la organización

J. *Vishing.*

Es una práctica criminal fraudulenta en donde se hace uso del Protocolo Voz sobre IP (VoIP) y la Ingeniería Social para engañar personas y obtener información delicada como puede ser información financiera o información útil para el robo de identidad. Es un delito similar al phising, pero a diferencia de éste, no ofrece un link para que la víctima se dirija a él, sino que le ofrece un número de teléfono al cual comunicarse. El término es una combinación de dos palabras en inglés "voice" (voz) y phishing.

**Contramedidas:* la mejor forma de prevenir el vishing es por medio del sentido común y el cuidado de nuestra información personal. Por ello al recibir llamadas de una supuesta entidad bancaria, hay que cerciorarse de la legitimidad de la misma antes de ofrecer información personal. Cuando existe necesidad de comunicarse con una institución bancaria o financiera, hay que hacerlo directamente a los números oficiales ofrecidos por ellos, y no por otros que se reciban por otros medios como mensaje de texto.

K. Social Networking.

Las redes sociales son un "paraíso" para los Ingenieros Sociales. Esta es la plataforma ideal para concretar el primer paso de la metodología del ataque: recopilar información de la víctima. Hoy en día, y puesto que las redes sociales son una tecnología nueva, hay poca cultura de la seguridad y poca educación sobre los peligros que estas involucran. En la mayoría de las redes sociales, los usuarios incautos muestran información como: nombres completos, dirección de residencia, lugar de trabajo, sus bagaje académico, su lista de amigos, sus vínculos familiares, sus preferencias políticas, su ideología, su religión, sus gustos, incluso el lugar en donde se encuentran en ese momento comiendo o bebiendo. La figura 8 muestra el incremento de uso en el tiempo.

**Contramedidas:* Para combatir los ataques que se generen a partir de las redes sociales o haciendo uso de la información contenida en ellas será necesario tener usuarios informados en temas de seguridad y comprometidos a seguir los buenos hábitos y prácticas para garantizar la seguridad personal y de la organización. Un programa detallado de entrenamiento sobre la seguridad de la información será siempre la mejor contramedida para evitar este tipo de ataques.

L. *Persuasión:*

Esta técnica consiste en tener la capacidad o habilidad para convencer a una persona mediante razones o argumentos, argumentos e ingeniosos para que piense de una determinada manera o haga cierta cosa.Es el proceso de guiar a la gente hacia la adopción de una idea, actitud, o la acción mediante significados racionales y simbólicos (aunque no siempre lógicos). Es una estrategia de resolución de los problemas que confía en "peticiones" más que en la coacción. Un Ingeniero social es un experto en laretórica. Como dijo Aristóteles: "la retórica es el arte de descubrir, en cada caso en particular, los medios adecuados para la persuasión".

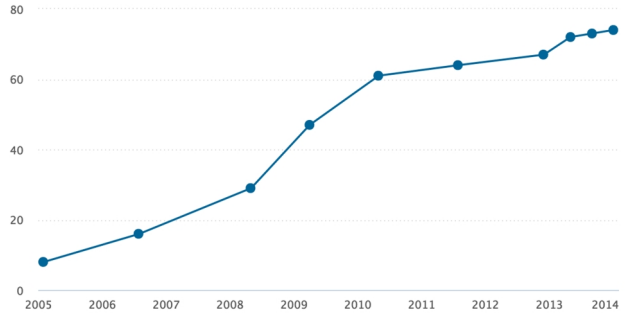


Fig. 8. Incremento del uso de las redes sociales en el tiempo.

**Contramedidas:* Para combatir este tipo de ataques será necesario tener usuarios informados en temas de seguridad y comprometidos a seguir los buenos hábitos y prácticas para garantizar la seguridad de la organización. Un programa detallado de entrenamiento sobre la seguridad de la información será siempre la mejor contramedida para evitar este tipo de ataques.

M. Pretexting.

Es el equivalente humano de phishing, donde alguien se hace pasar por una figura de autoridad o alguien de su confianza para obtener acceso a información. Puede tomar la forma de un miembro de soporte de TI falso con la necesidad de hacer el mantenimiento a un equipo, o un falso investigador para realizar una auditoría en la empresa. Alguien podría hacerse pasar por compañeros de trabajo, la policía, las autoridades fiscales u otras personas aparentemente legítimas con el fin de tener acceso a su computadora y a la información.

**Contramedidas:*para combatir este tipo de ataques es necesario que los empleados siempre sigan los buenos hábitos y políticas de seguridad que dictan verificar la identidad de cualquier persona que solicita acceso a los equipos, sistemas o información de la organización. Un programa detallado de entrenamiento sobre la seguridad de la información será siempre la mejor contramedida para evitar este tipo de ataques.

N. Quid Pro Quo.

Esta frase significa "algo por algo" y en seguridad de la información es un tipo de ataque que consiste en una solicitud de información a cambio de alguna compensación. Podría ser una camiseta gratis o acceso a un juego o servicio en línea a cambio de sus credenciales de acceso, o por ejemplo un "investigador" que pide la contraseña como parte de una encuesta a cambio de $ 100. Si suena demasiado bueno para ser verdad, probablemente es un ataque de quid pro quo.

**Contramedidas:* Para combatir este tipo de ataques será necesario tener usuarios informados en temas de seguridad y comprometidos a seguir los buenos hábitos y prácticas de seguridad. Un programa de entrenamiento sobre la seguridad de la información será siempre la mejor contramedida para evitar este tipo de ataques.

VIII. ESTUDIO Y ANÁLISIS DE VULNERABILIDAD A EMPRESAS SALVADOREÑAS.

A. Metodología.

Para realizar este estudio, se decidió llevar a cabo la recopilación de información por medio de dos herramientas: la encuesta y la entrevista personal. La encuesta consistió en 10 preguntas básicas sobre la conciencia del usuario en la seguridad de la información en sus organizaciones. Las preguntas estaban orientadas a determinar si el usuario es consciente de los peligros y riesgos, y que tanto interés existe de parte de el para aprender y educarse en el tema. Aquí tratamos de confirmar la hipótesis del trabajo en la cual se establece que el ser humano es el eslabón más débil de la cadena de seguridad de una organización. La parte de entrevistas se realizo con algunas de las personas encuestadas para profundizar más sobre su percepción sobre la seguridad de la información, y para conocer que tan acertadas eran las respuestas proporcionadas en las encuestas. Por ejemplo, algunas personas que respondieron que si conocían la manera de hacer una transacción electrónica segura, después de la entrevista era evidente que tenían poco o ningún conocimiento del asunto.

B. Descripción de empresas.

Siguiendo una convenio de privacidad con las empresas en estudio, no se revelan los nombres reales de las empresas en estudio, pero si su actividad y giro del negocio, el cual es lo fundamental para comprender el ámbito en que se desarrollaron las encuestas así como para la interpretación de sus resultados.

La primera organización en estudio es una empresa del sector eléctrico dedicada a la generación de energía la cual llamaremos Empresa Térmica S.A. La segunda organización es una empresa del sector de servicios dedicada a los juegos de azar que llamaremos Bingo S.A.

C. Tipo de empleados.

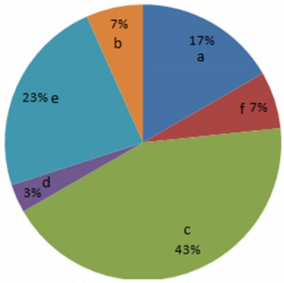
Durante el estudio de ambas organizaciones se decidió estudiar a los empleados que tuvieran contacto frecuente con personas externas a la organización. Se decidió dejar de lado personas con conocimientos técnicos de TI, ya que estos tienen ya un poco de conocimiento de las generalidades en temas de seguridad de la información, no así el empleado regular como el recepcionista, la cajera o un oficinista.

Para el caso de la Empresa Térmica S.A. se eligieron oficinistas regulares, recepcionista, encargado de la biblioteca y personal de servicio. Para el caso de la empresa Bingo S.A. se eligieron mayormente cajeras, las cuales tienen a su cargo el manejo del efectivo y las transacciones comerciales producto de sus actividades de los juegos de azar.

D. Resultados y Análisis.

Para los efectos de análisis mostraremos únicamente las preguntas más relevantes que muestran un panorama amplio de la realidad en la conciencia del usuario sobre los riesgos y los temas de seguridad, que ponen hoy por hoy en peligro las actividades y existencia de la organización.

*La pregunta #1 buscaba medir el nivel de conocimiento de las personas encuestadas sobre la manera apropiada de defenderse de ataques de Ingeniería Social, así como medir el conocimiento de sobre tratan este tipo de ataques. Decía: ¿Cual opción considera usted como la más efectiva contra los ataques de Ingeniería Social?

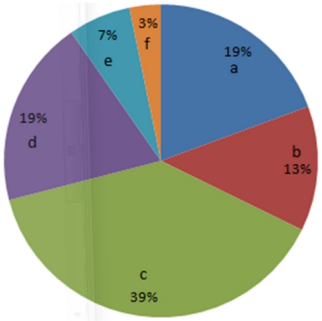


a. Antivirus.
b. Firewall.
c. Educación en Seguridad.
d. Antispyware.
e. Software de detección de intrusos.
f. Ninguno de los anteriores.

Fig. 9. Más del 50% de los encuestados ignoran la manera correcta de defenderse contra los ataques de Ingeniería Social.

En esta pregunta se observa que en general los encuestados tienen una buena idea de cuál es la mejor opción, sin embargo el resto que representa un 57% no tiene idea de cuál es la manera adecuada para abordar dichos ataques. Este elevado porcentaje es preocupante pues evidencia una gigantesca brecha de seguridad, y una gran oportunidad para los ingenieros sociales de penetrar la seguridad de estas empresas.

*La pregunta #2 buscaba conocer la percepción de los empleados sobre la probabilidad de ser víctima de espionaje industrial en su empresa, algo que revela el nivel de importancia que estos le dan a las posibles políticas de seguridad que tengan en sus organizaciones, esta decía: ¿Qué porcentaje de probabilidad considera usted que su organización puede ser víctima de espionaje industrial?



a. < 10%
b. Entre 10 % - 25%
c. Entre 25% - 50%
d. Entre 50% - 75%
e. Entre 75% - 90%
f. > 90%

Fig. 10. Solamente el 29% de los empleados en estudio consideran una alta probabilidad de espionaje industrial en su organización.

Los resultados confirman la manera relajada con que los empleados toman el espionaje industrial, tomando como lema el dicho que dice “los accidentes les ocurren a otras personas”. Aquí se evidencia que menos del 71% de los encuestados considera que su organización podría sufrir espionaje industrial, lo que significa que al no percibir o conocer la magnitud del daño potencial, estas personas no toman en serio cualquier medida de prevención que sus organizaciones posiblemente estén difundiendo. Cuando un empleado cree que no puede ser víctima de ataque no fomenta los procedimientos de seguridad y no se da a la tarea de informarse.

*La pregunta #4 buscaba conocer nivel de interés y la interacción de los usuarios con noticias o material educativo en seguridad de información. Decía: ¿Con que frecuencia lee usted artículos o noticias relacionados a ciberamenazas o temas de seguridad de la información?

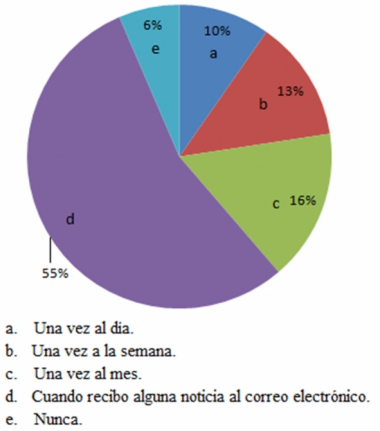


Fig. 11. El correo electrónico parece ser uno de los medios estratégicos para refrescar constantemente los temas del entrenamiento en seguridad.

Claramente se ve el poco interés de informase por parte de los usuarios. Solamente el 13% de los usuarios afirman leer contenido educativo en seguridad una vez a la semana. Mientras que un 32% te una poca o nula frecuencia de contacto con material educativo. Este porcentaje es suficientemente algo como para que un ingeniero social se las ingenie y burle todas las medidas de seguridad tecnológicas que tenga la organización. Basta 1 tan solo empleado, 1 tan solo clic en un vínculo malicioso para que un ciberatacante logre su objetivo. Llama la atención que más del 50% afirma leer el material sobre seguridad que recibe en su correo electrónico, lo que significa que este medio puede ser estratégico para mantener un entrenamiento de seguimiento en temas de seguridad de la información, algo que complemente al entrenamiento base que se debe diseñar.

*La pregunta #5 estaba orientada a comprender si el usuario era capaz de determinar si tiene responsabilidad en la seguridad de la información que maneja. Expresaba: ¿Quién considera usted que es el principal responsable de la seguridad de los activos del negocio, incluyendo la información en su computadora?

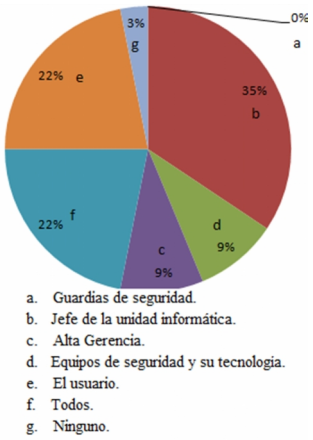


Fig. 12. Solamente un 22% combinado de los empleados responsabilidad de la seguridad como propia.

Esta pregunta arrojó un dato importante, 78% de los empleados encuestados no consideran la seguridad de la información como su responsabilidad. Estas personas creen que alguien más está a cargo y son los únicos responsables de cuidar ese activo de la organización, lo cual represente una gigantesca brecha de seguridad que solo puede ser combatida mediante una entrenamiento, una capacitación en temas de seguridad. El objetivo primordial aquí, es que todos los empleados lleguen a la comprensión de que todas las personas en la organización son responsables de la seguridad de la información, desde los guardias de seguridad, operadores de sistema, hasta la alta gerencia, y que resguardarla es parte primordial de sus actividades de trabajo.

*La pregunta #7 nos permitía conocer la permisividad de los privilegios que se le otorgan actualmente al usuario en las organizaciones en estudio, en este caso particular privilegios de instalación de software. ¿En algún momento usted ha instalado algún software gratuito (de libre uso) en su computadora personal o de trabajo?

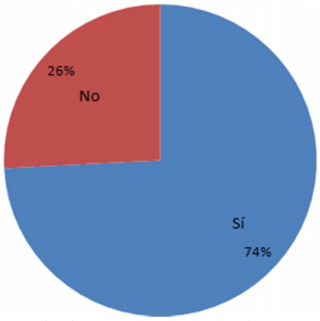


Fig. 13. Los resultados muestran que los empleados tienen privilegios de instalación inadecuados en sus equipos.

El análisis de estos resultados se complementó con las entrevistas en persona en donde se evidencio que la mayoría de las personas ha instalado software que no está autorizado por el departamento de TI en sus organizaciones. Aquí es necesario establecer la responsabilidad que tienen las personas de cumplir con las políticas de seguridad, así como establecer políticas fuertes desde el departamento de TI para minimizar los riesgos que provengan de la instalación de software de dudosa procedencia.

*Las preguntas #8, #9 y #10 buscaban investigar si el usuario se sentía capaz de realizar acciones online seguras, como comprar en un sitio web, navegar e interactuar en redes sociales de manera segura.

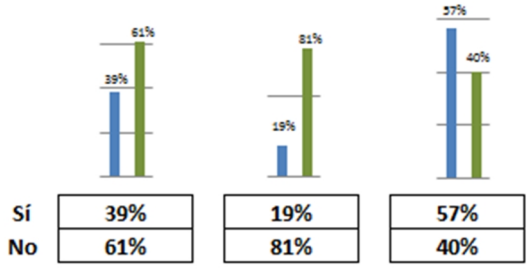


Fig. 14. Resultados de preguntas 8, 9 10.

Este análisis se complemento con las entrevistas en persona. Finalmente se evidencio que, aun cuando un buen número de personas consideraba que sus hábitos de navegación eran seguras, realmente desconocían muchas de las buenas prácticas o de los elementos que definen si una acción es segura o insegura. El problema con este grupo de personas es que, confiadamente realizan transacciones en línea y tienen un uso habitual en redes sociales, creyendo que son conocedores de los hábitos de seguridad que los protegen. Y cuando una persona cree estar seguro y no lo está, es cuando más fácil se le hace la tarea al ingeniero social para atacar y conseguir el acceso que desea.

IX. Planes de acción contra los ataques de ingeniería social

Existen medidas de prevención a todos los tipos de ataque que la Ingeniería Social utiliza. El primer paso es comprender y la conciencia del riesgo entre los encargados de la seguridad de la información. Sin embargo el mero hecho de comprender no garantiza la seguridad ya que las estadísticas muestran que la mayoría de los profesionales en seguridad de la información conocen y tienen conciencia de los riesgos.

En una organización, mantener y mejorar un programa de educación en temas de seguridad para los empleados es un factor clave [16]. Además del entrenamiento en temas de seguridad, los empleados siempre deben seguir procedimientos adecuados en cuanto a la divulgación de información [17].Los empleados deben ser entrenados para cuestionar cuando alguien está haciendo una petición de información y no deben dudar en pedir una identificación o credencial. Los empleados debe tratar la información en su organización como su fuera propia y asegurarse de informar a un supervisor cuando una solicitud de información parece fuera de lo normal [18], es necesario crean conciencia de la importancia de la seguridad de la información en la organización.

El Monitoreo y las pruebas continuas son formas adicionales para que las organizaciones puedan luchar en contra la Ingeniería Social. Monitorear constantemente los sistemas de seguridad de la empresa y la realización de pruebas internas basadas en la Ingeniería Social revelará los puntos vulnerables de una empresa [19]. Cuando ya se han identificado las vulnerabilidades, una organización entonces puede evaluar adecuadamente cómo se implementará una solución integral.

El entrenamiento en temas de seguridad puede ser reforzado haciendo cambios de roles para tener una dinámica mas interactiva para afianzar lo que han aprendido. También puede utilizarse el entrenamiento de tipo cascada para transmitir la información a todos los niveles.

A. Creación de un Programa de Entrenamiento y Concientización en Seguridad Informática a Empleados.

Elaborar un panfleto sobre las políticas o dirigir a los empleados a una página web de la intranet de la empresa no es en sí un programa de seguridad y concientización y no reduce ningún riesgo. La organización no solo debe asegurarse de desarrollar y elaborar políticas y reglas, plasmadas en documentos, sino también hacer un esfuerzo por hacer que los empleados que manejan la información corporativa, sigan y se interesen por las políticas. Así mismo, es importante que se comunique la intención y propósito detrás de cada política de seguridad, para que las personas no las sobrepasen por alguna conveniencia personal. La ignorancia será siempre la excusa de cualquier empleado, y la principal vulnerabilidad que explotará el ingeniero social. El objetivo de todo programa de seguridad es exhortar e influenciar a los empleados a cambiar su actitud y comportamiento para hacer su parte en la protección de la información de la organización. Una manera de hacerlo es explicando como el programa producirá beneficios no solo a la organización sino también de manera personal, ya que toda compañía tiene información de cada empleado, al proteger este tipo de información los empleados están protegiéndose a sí mismos.

El programa de entrenamiento debe tener un apoyo substancial de la alta gerencia, necesita llegar a cada empleado que tenga acceso a información sensible o a los sistemas informáticos de la empresa, debe de dársele seguimiento, debe ser revisado y actualizado constantemente sobre nuevas amenazas y vulnerabilidades.

**Objetivos.*

La directriz básica que debe tenerse en cuenta durante el desarrollo de un entrenamiento de seguridad de la información y el programa de concientización es que el programa tiene que centrarse en crear en todos los empleados la conciencia de que su organización podría estar bajo ataque en cualquier momento. Deben aprender que cada empleado desempeña un papel en la defensa contra cualquier intento de ganar acceso a los sistemas informáticos o de robar datos confidenciales. Puesto que la seguridad de información involucra tecnología, es muy fácil que los empleados consideren que el problema

está siendo controlado por firewalls u otros dispositivos tecnológicos como se mostró anteriormente el análisis hecho a dos empresas salvadoreñas [***]. Así que, uno de los principales objetivos del programa de seguridad debe ser concientizar a los empleados de que ellos son en realidad la primera línea de defensa necesaria para la protección en general de una organización. El programa de seguridad debe tener un supremo objetivo, más allá de elaborar e impartir reglas. La persona encargada debe tener en cuenta la fuerte tentación de los empleados, que algunas veces estando bajo estrés, tratan de sobre pasar las políticas de seguridad para entregar a tiempo sus responsabilidades.

La organización puede contar como exitoso su programa, si al finalizar el entrenamiento cada una de las personas involucradas están convencidas y motivadas por una simple noción: que la seguridad de la información es parte de su trabajo.

**Establecimiento del programa de entrenamiento y concientización.*

La persona responsable de diseñar el programa de seguridad de la información tiene que reconocer que esto no existe una estructura única para todos los proyectos. Por el contrario, la formación tiene que ser desarrollada para satisfacer las necesidades específicas de los diferentes grupos dentro de la empresa. Como mínimo, la mayoría de las empresas necesitan programas de formación adaptados a estos grupos distintos dentro de la organización: los gerentes; personal de TI; usuarios de computadoras; personal no técnico; auxiliares administrativos; recepcionistas; y guardias de seguridad.

Puesto que el personal de seguridad de una empresa normalmente no se espera que sea competente en el área de informática, excepto quizá de una manera muy limitada, no suelen ser considerados en el diseño de los entrenamientos de este tipo. Sin embargo, los ingenieros sociales pueden engañar a los guardias de seguridad u otras personas para ganar acceso a un edificio u oficina, o en la ejecución de una acción que da lugar a una intrusión informática. Aunque este tipo de empleados no necesitan un entrenamiento a fondo sobre las técnicas de Ingeniería Social, como el resto de empleados que están en contacto con los sistemas, no deben ser pasados por alto en el establecimiento del programa.

Los mejoresprogramas de capacitación en seguridad de la información deben informar y captar la atención y el entusiasmo de los alumnos.El objetivo debe ser hacer del programa de seguridad de la formación una experiencia atractiva e interactiva. Las técnicas pueden incluir una demostración de métodos de Ingeniería Social a través de juegos de roles; revisar periódicamente noticias en los medios de comunicación de ataques recientes a otras organizaciones menos afortunadas y discutir las formas en que podrían haber evitado la pérdida; o bien mostrar un video de seguridad que sea entretenido y educativo al mismo tiempo.

*Estructura del entrenamiento.

Un programa básico de capacitación en el tema de seguridad de la información debe ser desarrollado de tal manera que requiera que todos los empleados deban asistir. Los nuevos empleados deben ser obligados a asistir a la capacitación como parte de su inducción inicial. Se recomienda que no seproporcione a ningún empleado, sin distinción alguna, acceso a los equipos y sistemas de información hasta que haya asistido y comprendidolas reglas y políticas de seguridad básica.

Para las primeras sesiones del entrenamiento se recomiendan charlas cortas enfocadas primeramente en captar la atención de los asistentes para que mensajes cortos sean recordados. Aunque la naturaleza del material es que sea abundante, se recomienda fomentar la concientización y la motivación en conjunto con mensajes cortos y esenciales en lugar de jornadas largas de medio día, que dejan a los participantes del curso atiborrados con demasiada información que no podrán recordar.

El énfasis de estas sesiones debe ser la de transmitir una apreciación del daño potencial hacia la empresa y los empleados individualmente, a menos que todos los empleados sigan los buenos hábitos de trabajo de seguridad. Más importante que el aprendizaje sobre prácticas específicas de seguridad es el motivo que lleva a los empleados a aceptar la responsabilidad personal en la seguridad de la información. En situaciones en las que algunos empleados no puedan asistir fácilmente a sesiones de entrenamiento, la empresa debe considerar otras formas de instrucción y entrenamiento, tales como videos, capacitación basada en software, cursos en línea, o materiales escritos.

Después de la sesiones iníciales de charlas cortas, sesiones más largas deben ser diseñadas para educar a los empleados acerca de vulnerabilidades específicas y técnicas de ataque con respecto a su cargo o posición en la empresa. Charlas de actualización se deben llevar a cabo al menos una vez al año. La naturaleza de las amenazas y los métodos utilizados para explotar las vulnerabilidades de las personas es siempre cambiante, por lo que el contenido del programa debe mantenerse al día. Por otra parte, la conciencia y el estado de alerta de las personas disminuye con el tiempo, por esta razón las capacitaciones y entrenamientos deben repetirse a intervalos razonables para reforzar los principios de seguridad.

Los empleados que cambien de posiciones dentro de la organización para un trabajo que implique el acceso a sistemas de información o información sensible deben, por supuesto, deberán completar un programa de entrenamiento de seguridad adaptado a sus nuevas responsabilidades. Por ejemplo, si técnico en sistemas se convierte en un administrador de sistemas, o una recepcionista se convierte en un auxiliar administrativo, se requiere una nueva formación adaptada a estas nuevas posiciones.

**Contenido del curso de entrenamiento*

Casi cualquier ataque de Ingeniería Social podría ser frustrado si los empleados siguieran estos dos pasos fundamentales:

- Verificar la identidad de la persona que hacer la solicitud de información. ¿Es la persona solicitante quien dice ser?
- Verificar si la persona tiene autorización. ¿está esta persona autorizada para hacer esta solicitud?

Un programa de entrenamiento y concientización en seguridad de la información que aborda las vulnerabilidades humanas y la Ingeniería Social debería tener como mínimo lo siguiente:

- Una descripción de cómo los ciberdelincuentes usan la Ingeniería Social para engañar a las personas.
- Los métodos usados por los ingenieros sociales para conseguir sus objetivos.
- Como reconocer un posible ataque de Ingeniería Social.
- El procedimiento para manejar una solicitud de información sospechosa.
- EL lugar correcto para reportar intentos de ataques de Ingeniería Social o ataques realizados.
- La importancia de no dejarse manipular ante una solicitud sospechosa, aun cuando esta venga de alguien que alegue tener una posición importante en la compañía.
- El hecho de no confiar implícitamente en los demás sin antes hacer las verificaciones correspondientes, aun cuando el impulso natural del ser humano es dar siempre el beneficio de la duda.
- La importancia de verificar la identidad y autoridad de una persona solicitando información o realizar una acción.
- Procedimientos para proteger información sensible, incluyendo la familiaridad con el sistema de clasificación de información
- La ubicación de las políticas de seguridad y los procedimientos de la compañía, y su importancia en la protección de la información y los sistemas de la organización.
- Un resumen de las políticas de seguridad más importantes, y la explicación de su propósito. Por ejemplo como diseñar un password difícil de adivinar.
- El deber de cada empleado de cumplir con las políticas de seguridad, y las consecuencias de no cumplirlas.

Puesto que la Ingeniería Social involucra cierto grado de interacción humana, un atacante usara un sin número de maneras y tecnologías para alcanzar su objetivo. Por esta razón, un programa bien diseñado de entrenamiento y concientización incluirá y cubrirá los siguientes temas:

- Políticas de seguridad relacionadas con los passwords de computadoras y mensajes de voz en el teléfono.
- Procedimiento correcto para revelar información sensible o material confidencial de la organización.
- Política de uso del correo electrónico, incluyendo las buenas prácticas para salvaguardarse de ataques de código malicioso incluyendo todo tipo de malware.
- Requerimientos para la seguridad física como el uso de credenciales para los empleados.
- Cómo determinar la clasificación de la información, y las políticas de seguridad adecuadas para proteger la información sensible.
- La eliminación adecuada de documentos sensibles y medios informáticos que contienen, o que tuvieron en cualquier momento del pasado, materiales e información confidenciales.

**Pruebas*

La organización luego necesitará probar a los empleados sobre el aprendizaje de la información presentada en el entrenamiento del programa de seguridad, y esto se debe hacer antes de permitir cualquier acceso alos sistemas informáticos. Será necesario analizar los resultados de las pruebas para determinar las áreas del programa que necesitarán ser fortalecidas.

Se puede considerar la posibilidad de otorgar un certificado acreditativo de la realización del programa de seguridad de la información como una recompensa al empleado, con el objetivo de mantenerlo motivado. Se recomienda que al completar el programa se pida a cada empleado a firmar un acuerdo para cumplir con las políticas de seguridad y las buenas prácticas que se enseñan en el. Las investigaciones sugieren que una persona que hace el compromiso de firmar un acuerdo de este tipo es más probable que haga un esfuerzo extra por cumplir con los procedimientos.

*Seguimientoal programa de entrenamiento.

La mayoría de las personas son conscientes de que el aprendizaje, incluso sobre asuntos importantes, tiende a desvanecerse con el tiempo a menos que sea reforzado periódicamente. Debido a la importancia de mantener a los empleados al día sobre el tema de la defensa contra los ataques de Ingeniería Social, es necesario actualizar el programa y darle un seguimiento regularmente.

Uno de los métodos para mantener la seguridad en el pensamiento de los empleados es hacer la seguridad de la información una responsabilidad de trabajo específico para cada persona en la empresa. De lo contrario, existe una fuerte tendencia a sentir que la seguridad "no es mi trabajo", como se demuestro en el estudio hecho a empresas salvadoreñas anteriormente.

** Niveles de Entrenamiento*

Esta es una propuesta para seccionar los tipos de entrenamientos por niveles según el tipo de personas al cual va dirigido. Aun que este es un modelo de estructura, lo importante es hacer un análisis en la organización para tropicalizarlo según las necesidades. En algunas organizaciones más maduras se necesitaran quizá, un modelo más granular, en otras este modelo básico bastará.

1-Alto: Este nivel de entrenamiento representa el tipo de personas que están esperando ataques de Ingeniería Social y/o tienen los privilegios de hacer cambios significativos para volver la red inutilizable. A este nivel, es donde se concentra la mayor cantidad de información sensible para poder hacer grandes ataques, es por eso que este grupo de personas debe ser la más altamente entrenada para generar estrategias y tácticas a seguir para garantizar la seguridad de los activos de la empresa. Un ejemplo de estos usuarios son los técnicos de soporte de TI ya que ellos se dedican a dar soporte y ayudar todos los días a los usuarios finales y poseen una cantidad de privilegios de red que típicamente incluyen agregar o remover usuarios en el controlador de dominio así como cambiar y restablecer sus contraseñas [21].

2-Medio: Este nivel representa personas quien podría tener contacto con el público en general. Este grupo de personas pueden no tener autoridad o privilegios para hacer cambios en la red, pero si pueden correr comandos en una consola o trasladarse a una máquina y hacer un sin número de cosas desde ahí. El entrenamiento en este caso debe ir enfocado en solicitar siempre la identidad de las personas y confirmar la autenticidad antes de dar cualquier información o hacer cualquier favor [21].

3-Bajo: Este grupo involucra a personas que tienen poco o ningún acceso a la red. Aquí hablamos del personal de seguridad y porteros. El entrenamiento en este nivel debe incluir una explicación de todas las tácticas de la Ingeniería Social, y en alguna situación podría enfatizarse en no dejar ingresar a la organización a personas no autorizadas después de las horas laborales, así como evitar hacer favores a cualquier persona por ninguna circunstancia. En este nivel se pueden obviar algunas tácticas que pueden no ser aplicables a este grupo de usuarios [21].

Una empresa deberá desarrollar un plan de entrenamiento en temas de seguridad que se ajuste a sus necesidades particulares pues no existen dos organizaciones idénticas. Para los empleados que trabajan en aéreas que no son usualmente atacadas, una estrategia baja-media puede ser suficiente, sin embargo es necesario no olvidar reforzar y darle continuidad al entrenamiento que se les proporciona.

Una buena estrategia de entrenamiento en temas de Ingeniería Social puede rápidamente desvanecerse o durar poco tiempo si no se le da la continuidad necesaria, por ejemplo, una buena práctica es enviar correos cortos o postear en muros donde todos los empleados puedan ver los boletines informativos de la empresa. Se mencionan algunos tipos de entrenamientos sugeridos según el rol del personal dentro de la organización.

- *Helpdesk:* un técnico de soporte debe estar altamente entrenado para frustrar cualquier intento de ataque de Ingeniería Social. Generalmente los técnicos de soporte siempre están recibiendo solicitudes y requerimientos por email, mensajes instantáneos, por teléfono o en persona y un ingeniero social podría persuadir al técnico de soporte para hacerle creer que es un usuario legítimo que necesita alguna clase de ayuda. La tarea principal de un técnico de soporte es –ayudar- y eso es exactamente lo que está buscando un ingeniero social, una persona con la voluntad de ayudar. Los técnicos de soporte deben de ser entrenados para ser lo suficientemente amables y a la vez actuar con prudencia y escepticismo, actuar con buen juicio antes de actuar y ayudar a un usuario. El técnico debe de hacerse preguntas pertinentes sobre si el usuario es realmente legítimo y si a la vez, necesito los privilegios y tipo de ayuda que solicita.

- *Administrador de T.I.:* Un administrador de TI puede que no reciba muchas llamadas de soporte, pero aun así es uno de los principales objetivos de ataques pues es quien posee los privilegios para controlar la red.Si existe una persona a la cual un ingeniero social le gustaría influir para que corra comandos, envié y transfiera información por la red es precisamente un Administrador de T.I. Esta es la razón por la que esta persona debe tener un gran entrenamiento para detectar y evitar ataques de Ingeniería Social. Los administradores de red suelen estar másconscientes de los tipos de ataques a nivel técnico pues ellos entienden lo complejo y destructivo que un comando puede ser. Sin embargo ellos aún son vulnerables cuando los ataques tienen que ver con técnicas como "solicitar o simplemente pedir" información mediante una llamada telefónica.

- *Recepcionista:* Una recepcionista es un término muy amplio cuando se trata de responsabilidades y un plan de entrenamiento deberá que ser hecho a la medida para adaptarse a su trabajo. Una recepcionista está en la puerta principal de una empresa y contesta llamadas durante todo el día, así quedebería ser entrenada más ampliamente en tácticas las tácticas de persuasión y las tácticas telefónicas que usan los ingenieros sociales. En el caso de una secretaria personal de un director general que hace un montón de trabajo en línea y mensajes de correo electrónico, probablemente debería ser capacitado más en las tácticas de Ingeniería Social en línea, así como en las técnicas mediante llamadas telefónicas en la que alguien necesita un favor, porque el director general les dijo que podían llamar a la secretaria para que le proporcionara información. Dependiendo de la función de trabajo, una cantidad moderada de entrenamiento debería ser suficiente para una recepcionista.

- *Tele trabajador:* el entrenamiento de este tipo de usuario debe ser de mediano a alto, simplemente porque su red interna de trabajo en casa es más simple, y eso la hace más vulnerable de atacar y así comprometer la red de la empresa remotamente. A la vez, le da más probabilidades al atacante de mantenerse anónimo pues no existen equipos de seguridad robustos en este extremo de la red.

- *Departamento de Recursos Humanos:*R.R. H.H. administra toda la información personal de los empleados de una empresa. Aun cuando no todos los empleados están interesados en proteger activamente la información empresarial si deberían estar interesados en proteger su propia información personal para evitar su robo. El ejemplo que proyecte R.R.H.H. en el cuido de la información personal puede influir grandemente en los empleados a que hagan lo mismo con la información empresarial. Cuando el personal de este departamento se ponga en contacto con otros departamentos dentro y fuera de la empresa, debe seguir procedimientos claros y definidos para garantizar que la información se está enviando a la persona correcta y deben existir maneras de verificar la identidad de la persona solicitante. Los empleados de R.R.H.H. deben ser altamente entrenados para abordar a las personas que llaman solicitando información personal como sueldos, descuentos en planillas, referencias personales, cargos, etc., quienes dicen representar a instituciones financieras, bancos u otras organizaciones para gestionar algún producto oservicio al empleado.

- *Departamento de I+D*: Aun cuando este departamento no está en contacto directo con las personas fuera de la organización, no contesta llamadas telefónicas o una gran cantidad de correos, con un objetivo importante para los ingenieros sociales para llevar a cabo espionaje industrial a la organización. Este departamento debe tener tecnología de seguridad informática y al menos tener un entrenamiento moderado para conocer las prácticas de engaño que existen con el objetivo de sobrepasar las medidas de seguridad e ingresar a los servidores.

- *Ejecutivos y Directores de Empresas*: Los ejecutivos pueden variar mucho, unos necesitaran más entrenamiento que otros. Algunos ejecutivos simplemente no querrán ser molestados con este tema. Sin embargo es importante saber transmitir la idea que los ataques de Ingeniería Social involucran a toda la empresa y pueden tocar sus intereses directos. Generalmente un entrenamiento moderado es suficiente para los directos y ejecutivos, esto puede variar depende del rol que este tenga dentro de la organización.

B. Elaboración de Políticas de Seguridad Corporativas

En esta parte del trabajo se aborda la parte de la elaboración de políticas específicas destinadas a minimizar el riesgo de una empresa con respecto a los ataques de Ingeniería Social. Las políticas abordan los ataques que se no basan estrictamente en la explotación de vulnerabilidades técnicas, sino más bien en el uso de algún tipo de pretexto o artimaña para engañar a un empleado de confianza que provee información o realiza una acción que da acceso al atacante información sensible o a los sistemas informáticos de la empresa y la red.

1. *¿Qué hay en una Política de Seguridad?*

Las políticas de seguridad son instrucciones claras que proporcionan las pautas de comportamiento de los empleados para la protección de la información, y son un elemento fundamental en el desarrollo de controles eficaces para contrarrestar las potenciales amenazas de seguridad. Estas políticas son aún más significativas cuando tratan de prevenir y detectar ataques de Ingeniería Social.

Los controles de seguridad efectivos se implementan mediante la capacitación de los empleados con las políticas y procedimientos bien documentados. Sin embargo, es importante señalar que las políticas de seguridad, incluso si se siguen religiosamente por todos los empleados, no están garantizadas para prevenir todos los ataques de Ingeniería Social. Más bien, el objetivo razonable es siempre para mitigar el riesgo a un nivel aceptable. Las políticas expuestas a continuación no son estrictamente diseñadas solamente para ataques de Ingeniería Social, pero todas tratan la mayoría de las técnicas usadas en un ataque de Ingeniería Social.

2. *¿Cómo Usar las Políticas?*

Cada organización encargada de elaborar sus políticas de seguridad debe comprender que estas son únicas, y su elaboración dependerá de su ambiente, sector, requerimientos legales, cultura organizacional, sistemas informáticos usados y objetivos estratégicos particulares.

La rigurosidad de las políticas dependerá del tamaño de la organización. Por ejemplo, en una empresa donde hay pocos empleados, con una sola sucursal, y donde se conocen unos a otros, no deben de preocuparse tanto sobre la posibilidad de que un atacante llame para hacerse pasar por uno de sus empleados. Así mismo, una organización con una cultura relajada podrá adoptar solamente aquellas políticas que requiera para cumplir con sus objetivos estratégicos.

Aquí solo presentamos un sub-set de políticas, enfocadas y consideradas fundamentales para el área de TI.

3. *Clasificación de Datos.*

Una política de clasificación de datos es fundamental para proteger los activos de información de una organización, y establece categorías por las que debe regirse la divulgación de información sensible. Esta política proporciona un marco de referencia para la protección de la información corporativa al hacer a todos los empleados conscientes del nivel de sensibilidad de cada categoría de información. La información debe separarse en niveles de clasificación en función de su sensibilidad y confidencialidad. Para empresas medianas a grandes, estas 4 clasificaciones, que se mencionan a continuación, cumplen apropiadamente los requerimientos, para luego usarse en las políticas:

- Confidencial: esta categoría de información es la más sensible. La información confidencial es para uso solamente dentro de la organización. En la mayoría de los casos, sólo debe ser compartida con un número muy limitado de personas con una necesidad absoluta para conocerla. La naturaleza de la información confidencial es tal que cualquier revelación no autorizada podría afectar gravemente a la organización, sus accionistas, sus socios de negocios, y/o sus clientes.

  Ejemplos de información confidencial generalmente caen en una de estas categorías: información referente a secretos de negocio, patentes, códigos fuentes, especificaciones técnicas y de funcionamiento de equipos clave o información sobre productos que pueda ser usado como una ventaja competitiva por la competencia. Información sobre estrategias de mercadeo y finanzas no reveladas al público, así como cualquier otro tipo de información que sea vital para la operación del negocio, como su planeación estratégica.

- Privada: esta categoría cubre la información de carácter personal que se destina para uso exclusivo dentro de la organización. Cualquier divulgación no autorizada de esta clase de información podría afectar seriamente a los empleados o la empresa si fuese obtenida por personas no autorizadas (especialmente los ingenieros sociales).

  Ejemplos de información privada incluyenel historial clínico de los empleados, beneficios en las pólizas de salud, información de cuentas bancarias, historial de sueldo, o cualquier otra información que identifique al personal y que no es de conocimiento público.

- Interna: esta categoría de información se puede proporcionar gratuitamente a todas las personas empleadas por la organización. Por lo general, no se espera que la divulgación no autorizada de información interna para causar daños graves a la empresa, sus accionistas, sus socios, sus clientes o sus empleados. Sin embargo, las personas expertas en técnicas de Ingeniería Social pueden usar esta información para hacerse pasar por un empleado, contratista o proveedor autorizado para engañar incautos personal que proporcione información más sensible que daría lugar a un acceso no autorizado a los sistemas informáticos corporativos.

  Un acuerdo de confidencialidad debe ser firmado antes de que la información interna pueda ser revelada a terceros, como a los proveedores, contratistas, empresas asociadas, etc. La información interna generalmente incluye cualquier cosa usada para la actividad empresarial diaria que no debe ser revelada al público, como gráficos corporativos de organización, números de acceso telefónico de red, nombres internos del sistema, procedimientos de acceso remoto, códigos de centros de costo, etc.

- Publica: esta es la información que se ha diseñado específicamente para el público en general. Este tipo de información se puede distribuir libremente a cualquier persona, como comunicados de prensa, información de contacto de servicio al cliente, o folletos de productos. Hay que tener en cuenta que cualquier información no designada como pública debería ser tratada como información sensible.

Para los efectos de las políticas mencionadas a continuación, una persona *no verificada* es alguien a quien el empleado no conoce personalmente o que sepa que es un empleado activo o con los privilegios de acceso a la información, o alguien que no ha sido avalado por un tercero de confianza. Una *persona de confianza* es una persona se conoce cara a cara o un empleado de la compañía, un cliente o un consultor de la empresa con los privilegios adecuados para tener acceso a la información. Una persona de confianza también puede ser un empleado de una empresa que tiene una relación ya establecida, con su empresa.

4. *Procedimientos de Verificación y Autorización.*

Los ingenieros sociales suelen utilizar tácticas engañosas para acceder u obtener información confidencial de la empresa haciéndose pasar por empleados legítimos, contratistas, proveedores o socios de negocios.Para mantener la seguridad de la información eficaz, un empleado que reciba un requerimiento de realizar una acción o proporcionar información sensible debe identificar a la persona que llama y verificar sus privilegios antes de conceder una solicitud.

- *Requerimiento de una persona de confianza:* la condición para proveer información a este tipo de persona es que la organización mantiene como empleado activo a la persona que realiza la solicitud de información, o que la persona tiene una relación con la organización. Luego, es necesario verificar que la persona solicitante tenga una necesidad real de saber la información y si tiene los privilegios adecuados para conocerla.

- *Requerimiento de una persona no verificada:* cuando exista una solicitud de una persona no verificada, es necesario hacer una verificación razonable para conocer si esta persona tiene privilegios para solicitar esta información o acción. Esto se realiza mediante tres pasos o casos:

  -*Paso uno, verificar que la persona sea quien afirma ser:* será necesario tener tecnologías como caller's ID para poder identificar a la persona que llama. Para verificar la autenticidad de la llamada se puede devolver la llamada hacia el número oficial de la lista de contactos de la organización. Validar a una persona a través de un tercero es una buena práctica, aunque siempre en estos casos hay que tener constancia que la tercer persona está activa en la empresa, y una manera de hacerlo es consultarlo con su jefe o supervisor inmediato.
  Para la comunicación por correo electrónico, será necesario solicitar que el mensaje venga firmado electrónicamente. En el caso de solicitudes en persona siempre debe de verificarse las credenciales físicas de la persona solicitante.

  -*Paso dos, determinar si la persona es un empleado activo o una persona con una relación de confianza con la organización:* antes de revelar cualquier información será necesario verificar si la persona está autorizada para recibir y conocer este tipo de información. Esto se puede hacer indagando en el departamento o con el supervisor de la persona solicitante. En los sistemas electrónicos, una base de datos con la información de privilegios será una gran herramienta para conocer quien tiene acceso y que información de la compañía. Para verificar si la persona es un empleado activo y a que área pertenece será necesario utilizar un sistema de RRHH para activamente, realizar la verificación de manera eficaz.

-*Paso tres: determinar si la persona tiene la autorización para recibir la información, o de solicitar una acción:* Una vez se ha verificado la autenticidad de la persona es necesario saber si está autorizado para tener acceso a la información solicitante, por ejemplo, si un empleado del área de mercadeo solicita información financiera de empresa, esto ya debería levantar sospecha y la única manera de verificarlo seria mediante el sistema informático que tenga usuarios y privilegios.
Una empresa puede proporcionar un acceso fácil a la información de autorización mediante la publicación de listas que determinen que empleados tienen derecho a que información. Estas listas pueden ser organizadas en términos de posiciones, departamentos, grupos de trabajo, y las responsabilidades de los empleados o alguna combinación de estas. Tendrá que ser mantenida en la línea y actualizada y proporcionar un acceso rápido a la información de autorización.

5. *Políticas de Tecnología de la Información.*

El departamento de tecnología de la información de cualquier empresa tiene una necesidad muy especial por las políticas de seguridad que le ayudan a proteger los activos de información de la organización. En este trabajo se mencionan solo algunos ejemplos de políticas divididas en cuatro aéreas: General, Help Desk, Administradores y Operadores de Equipos.

- Generales.

  1-Politica de información de contacto para Staff de TI: números de teléfono y direcciones de correo electrónico no deberán ser reveladas a ninguna persona excepto ante un requerimiento oficial.

  Propósito: se busca que esta información no sea explotada por un ingeniero social. Al revelar solo información como un número general o un correo electrónico genérico se bloquea al ingeniero social para que contacte directamente a personal de TI.

  2-Politica de soporte técnico: todos los requerimientos de soporte técnico deben ser referidos al grupo que se encarga de este tipo de solicitudes.

  Propósito:Los ingenieros sociales pueden intentar dirigir sus ataquesa personal de TI que no manejan habitualmente problemas de soporte técnico, y que pueden no estar al tanto de los procedimientos de seguridad al atender estas solicitudes.

- Help Desk.

  *3-Politica de procedimiento para soporte remoto:*el personal de soporte técnico no deben divulgar datos o instrucciones en materia de acceso remoto, incluidos los puntos de acceso a la red externa o números de acceso telefónico, a menos que elsolicitantehaya sido: a) un empleado verificado y con autorización de recibir esa información, b) una persona verificada para conectarse a la red remota como un usuario externo. A menos que la persona sea conocida en persona, se deberá seguir los tres pasos de verificación detallados anteriormente.

  Propósito: El personal de soporte técnico es a menudo un objetivo primordial para un ingeniero social, pues la naturaleza de su trabajo es ayudar a los usuarios con problemas relacionados con los sistemas informáticos, y debido a que por lo general ellos tienen privilegios elevados del sistema. Todo el personal de soporte técnico debe estar capacitado para actuar como un firewall humano para evitar la divulgación no autorizada de información que pueda ayudar apersonas no autorizadasa tener acceso arecursos de la empresa.

4-Politica de restauración de passwords: el password de una cuenta de usuario podrá ser restaurada solamente por solicitud del usuario de la cuenta.

Propósito: La táctica más común de los ingenieros sociales es lograr que una cuenta de otra persona sea reseteada. En este caso el atacante finge que el usuario ha perdido u olvidado el password. Para reducir el riesgo de este tipo de ataques, todo el personal de TI debe llamar y contactar directamente al usuario que solicita un restablecimiento de password, antes de ejecutar cualquier acción. El número de teléfono al que contacta debe ser tomado de la lista oficial provista por la organización y no ser provisto por el solicitante.

*5-Política de cambio de privilegios de acceso:*todas las solicitudes para elevarlos privilegiosde un usuarioo delos derechos de accesodeben de ser aprobadospor escritopor el jefedeltitular de la cuenta. Cuando los cambios se hayan realizado se debe informar por medio del correo electrónico corporativo oficial al jefe solicitante.

Propósito: una vez un atacante ha comprometido una cuenta de usuario el siguiente paso será elevar los privilegios de esta cuenta para para tener más control sobre el sistema informático vulnerado. Si el atacante tiene conocimiento del proceso de autorización puede engañar y perpetrar solicitud falsa mediante correo electrónico, fax o llamada telefónica.

*6-Politica para autorización y creación de nueva cuenta:*la solicitud de creación de una nueva cuenta para un nuevo empleado contratista debe ser hecha por escrito y firmada por el jefe de la persona a quien se creara la cuenta, o en su defecto por medio de un correo electrónico firmado digitalmente. Este requerimiento también debe ser confirmado enviando un correo por medio del correo institucional al jefe peticionario.

Propósito: Debido a que los passwords y otra información útil es usada para vulnerar los sistemas y tener acceso no autorizado, son los objetivos más comunes de los atacantes. Po esta razón las precauciones que deben tomarse deben ser especiales. La intención de esta política es prevenir que un intruso suplante a un empleado o jefe legítimo para solicitar creación de nuevas cuentas.

7-Politica para la entrega de nuevos passwords: Los nuevos passwords deben ser administrados como información confidencial, y entregados por medios seguros incluidos en persona, contra firma de entrega, o servicio de encomienda cuando el usuario se encuentre en otra sede.

Propósito: El correo interno de la compañía puede ser utilizado aunque siempre será preferible que los documentos para la entrega de passwords se hagan en sobres seguros que cubra la totalidad del contenido del mismo.

8-Politica para la deshabilitación de una cuenta: Antes de deshabilitar la cuenta de un usuario, se debe solicitar una verificación por escrita, física o digital, de que el requerimiento proviene de una persona autorizada.
Propósito: el propósito de esta política es prevenir que un atacante solicite de manera fraudulenta la deshabilitación de una cuenta para luego, llamar al usuario de la cuenta bloqueado tratando de "solucionar" el problema. Cuando un usuario percibe que quien llama tiene ya conocimiento de su problema técnico estará más propenso a dar información como su usuario y password en el proceso de resolución de problemas.

9-Política para deshabilitar puertos de red y dispositivos: ningún empleado deberá deshabilitar ningún tipo de equipo de red o puerto solicitado por alguna persona no verificada de afirme ser de soporte técnico.

Propósito: el propósito de esta política es prevenir que un atacante detenga el servicio de un equipo de red o un puerto especifico, para luego, llamar a algún usuario con problemas de red para "solucionar" el problema. Cuando un usuario percibe que quien llama tiene ya conocimiento de su problema técnico estará más propenso a dar información como su usuario y password en el proceso de resolución de problemas.

10-Política de acceso a la red inalámbrica: ningún empleado debe revelar los procedimientos o pasos para acceder a la red y s inalámbricos a ninguna persona que no esté autorizada.

Propósito: Siempre se debe de verificar que la persona solicitante sea una persona autorizada para conectarse a la red, antes de conceder las credenciales y pasos para conectarse.

- Administración de equipos.

11-Politica para cambio general de derechos de acceso: las solicitudes para cambiar los derechos de acceso globales asociados con un perfil o usuario de trabajo debe ser aprobado por el personal asignado para la responsabilidad de gestionar los derechos de acceso en la red corporativa.

Propósito: el personal autorizado para cambiar privilegios determinará antes de realizarlos si los cambios pudieran afectar la seguridad de la información. Si fuera así, el solicitante asumirá la responsabilidad y se harán los cambios solicitados.

12-Política para solicitud de acceso remoto: todo acceso remoto será concedido solamente a aquellos empleados que demuestren que tiene una necesidad de acceder a los sistemas y red corporativa desde fuera de ella.

Propósito: cuando se limitan las personas que pueden acceder remotamente a aquellas que tiene una explicita necesidad de conectarse desde afuera de la organización, se reduce también el riesgo y la administración de los usuarios con estos privilegios. Entre menos personas existan con privilegios de acceso, menos objetivos de ataque tendrá un ingeniero social.

13-Política para restauración de passwords de cuentas privilegiadas: una solicitud de restauración de una contraseña de una cuenta privilegiada debe ser aprobada por el administrador del sistema o administrador responsable del equipo en cual existe la cuenta. La nueva contraseña se debe enviar a través del correo interno de la empresa o entregarse en persona.

Propósito: las cuentas de administrador tienen acceso a todos los recursos del sistema y a archivos almacenados en la computadora. Naturalmente, estas cuentas merecen la mayor protección posible.

*14-Política de soporte remoto:*ninguna personal de soporte técnico remoto puede dar ninguna información de acceso remoto o permitirle tener acceso a cualquier sistema de la compañía o dispositivos relacionados sin la verificación de identidad y autorización de realizar tales servicios. Si se requiere tener acceso remoto por soporte de hardware o software, la contraseña dela cuenta usada por el técnico de soporte se debe cambiar inmediatamente después de que los servicios del técnico se han completado.

Propósito: los atacantes se pueden hacer pasar por técnicos de soporte remoto para ganar acceso a la red corporativa. Por lo tanto, es esencial que la identidad del técnico de soporte se verifique además de su autorización para realizar cualquier trabajo en el sistema. Además, el acceso en el sistema se debe cerrar una vez que el trabajo se haya realizado.

- Operación de Equipos.

*15-Politica para ingresar comandos o correr programas:*el personal operativo de los equipos de cómputo no deberá ingresar ni correr ningún comando cuando alguien lo solicite y esta persona no sea verificada. Si surge una necesidad de que la persona no verificada necesita correr un comando, este deberá ser aprobado por el supervisor o jefe de área.

Propósito: los empleados operadores de computadoras son objetivos muy comunes para los ingenieros sociales, puesto que sus cargos tienen cuentas con privilegios elevados, y estos esperan que estos empleados tengan menos conocimientos y experiencia sobre procedimientos de seguridad en comparación con los empleados de TI.

16-Política para trabajadores con cuentas de privilegios elevados: los empleados con cuentas especiales de privilegios elevados no deberán proveer asistencia e información a ninguna persona no verificada. En particular esto se refiere a no proveer ayuda en el ámbito computacional, accesos a bases de datos de la organización, bajar software, o revelar nombres del personal de TI que tengan privilegios de acceso remoto.

Propósito: los ingenieros sociales siempre tienen como objetivos a empleados que tengan cuentas con privilegios elevados. La intención de esta política es dirigir al personal de TI todas las llamadas que puedan representar ataques de ingenieros sociales para que sean manejadas segura y exitosamente.

*17-Politica para información interna de sistemas:*el equipo de TI nunca debe revelar cualquier información que tenga que ver con los sistemas informáticos o relacionados con dispositivos sin identificar primero al solicitante.

Propósito: los intrusos informáticos suelen contactar a los operadores de equipos de cómputo para para obtener información valiosa como procedimientos de acceso a sistemas, acceso remoto, ip's públicas para VNP's, los cuales son información substancia para un atacante.

18-Política para revelación de passwords: los usuarios del equipo de cómputo y sistemas nunca deben revelar sus passwords, sin el consentimiento del gerente de tecnología de la información.

Propósito: en términos generales, al revelar cualquier password a otras personas está estrictamente prohibido. Esta política reconoce que en algunas ocasiones existe la necesidad de revelarlas a terceras personas cuando sea necesario, pero esta excepción debe ser aprobada por el gerente de TI.

19-Política de medios electrónicos: Todos los medios electrónicos que contengan información privada deben estar resguardados físicamente en un lugar seguro.

Propósito: el propósito de esta política es resguardar y evitar el robo de medios electrónicos que contengan información sensible de la organización.

20-Política de backup: el personal operativo debe guardar los dispositivos y/o medias de backup en una locación segura de la empresa o fuera de ella.

Propósito: Los medios de backup son objetivos de los intrusos informáticos. Un atacante no perderá tiempo tratando de burlar un sistema de seguridad o la red cuando el eslabón más débil pueden ser los dispositivos o medias de back que no están asegurados físicamente. Cuando un medio de backup es robado, toda la información contenida está comprometida. Una buena práctica es cifrar la información contenida en los medios de backup.

X. CONCLUSIONES

Los ataques de Ingeniería Social están siendo usados más frecuentemente pues cada vez más y más la tecnología aplicada a los sistemas se vuelve más robusta. La cadena de seguridad se rompe siempre por el eslabón más débil y los ingenieros sociales están atacando al ser humano con el objetivo de llegar a los sistemas de las organizaciones de una manera más fácil. Una vez el atacante puede identificar una víctima y la engaña, la red y los sistemas están comprometidos y el atacante puede usar muchas herramientas tecnológicas para robar y hacer daño a la organización. Actualmente la manera más eficaz de usar la Ingeniería Social es combinándola con tecnología, pues una vez ingresando a la red o sistema por un error humano, la tecnología se encarga de hacer el resto para él atacante. Muchos casos famosos de

pérdida de información comenzaron con un ataque de Ingeniería Social, como el caso de SONY [22], y es por esta razón que el primer paso para fortalecer la seguridad en esta área es estar consciente del peligro que esto involucra, mediante una evaluación de vulnerabilidad en el tema de Ingeniería Social en la organización. Luego será necesario elaborar un plan de educación en seguridad informática e Ingeniería Social para cada uno de los grupos de interés de la empresa, que como hemos visto en este estudio es única para cada organización. Luego, la elaboración de las políticas es fundamental para que cada empleado en sepa la manera de actuar, de una manera coherente y coordinada ante cada situación, reduciendo la incertidumbre y ambigüedad. El compromiso de todos los elementos de una organización, la continua capacitación y mejora del programa de educación es la única herramienta conocida para evitar el engaño, las tretas y el timo las personas para la obtención de información de manera ilícita. La seguridad de la información es tarea de todos, desde el guardia de seguridad hasta el CEO de la organización.

Cuadro de Resumen de Ataques y Contramedidas

ATAQUE	CONTRAMEDIDA
Shoulder Surfing	Mirar y estar consciente de las personas a su alrededor, y no permita que vean su pin o password.
Dumpster Diving	Destruir el material físico sensible en trituradora. Destruir el material digital haciendo un "wiping" a las particiones y volúmenes.
Phishing	Verificar la autenticidad del remitente. No contestar información personal a este tipo de correos. Reportarlo al Staff de TI.
El usuario importante	Tener claras y definidas las políticas de revelación de información. Difundir y poner en práctica dicha política.
Ingeniería Social Inversa	Tener claras y definidas las políticas de revelación de información. Si un empleado es completamente consiente de las políticas de seguridad, siempre estará atengo ante cualquier solicitud maliciosa de información.
Baiting	Tener usuarios informados en temas de seguridad y comprometidos a seguir los buenos hábitos y prácticas para garantizar la seguridad de la organización.
Generar una situación de hostilidad	Programa detallado de entrenamiento sobre la seguridad de la información será siempre la mejor contramedida para evitar este tipo de ataques.
Lenguaje corporal.	Para detener este tipo de ataque es necesario un programa de entrenamiento sobre la seguridad de la información, y políticas claras sobre cómo responder ante actos sospechosos.
Piggybacks Rides/Tailgating	Deber ser un hábito de todos los empleados solicitar la identificación en cualquier circunstancia. Seguir siempre las políticas de verificación de usuarios.
Vishing	Programa de entrenamiento sobre la seguridad de la información para identificar llamadas sospechosas. Seguir siempre las políticas de verificación de usuarios.
Social Networking	Tener usuarios informados en temas de seguridad y comprometidos a seguir los buenos hábitos y prácticas de comportamiento en las redes sociales para garantizar la seguridad personal y de la organización.
Persuasión	Para detener este tipo de ataque es necesario un programa de entrenamiento sobre la seguridad de la información, y políticas claras sobre cómo responder ante actos sospechosos.
Pretexting.	Programa de educación y entrenamiento a empleados en temas de seguridad y políticas claras sobre relevación de información.
Quid Pro Quo	Empleados comprometidos con la política de seguridad y revelación de información. Un programa de entrenamiento será siempre la mejor medida preventiva.

REFERENCIAS

[1] Kristian Beckers, Leanid Krautsevich, Artsiom Yautsiukhin, "Analysis of Social Engineering Threats with Attack Graphs". Pisa, Italy. The Ruhr Institute for Software Technology – University of Duisburg-Ess, 2013.

[2] Kevin Mitnick, William L. Simon, "El eslabón mas débil de la seguridad". USA. El Arte del Engaño. 2002

[3] Devin Luco, "The Art of Social Engineering", Seattle, USA. ASA Risk Consultants, 2013.

[4] Malcom Allen, "Social Engineering: A Means To Violate A Computer System", , USA. SANS Institute InfoSec Reading Room2007.

[5] "The risk of social engineering on information security: a survey of it professionals", Dimensional Research &CheckPoint, California, USA. 2011.

[6] Kristian Beckers, Leanid Krautsevich, Artsiom Yautsiukhin, "Analysis of Social Engineering Threats with Attack Graphs". Pisa, Italy. The Ruhr Institute for Software Technology – University of Duisburg-Ess, 2013.

[7] Goodchild, Joan. "Social Engineering: The Basics." CSO Security and Risk. 20 Dec 2012. Web. Apr. 2013.

[8] Goodchild, n. pag.

[9] Goodchild, n. pag.

[10] Goodchild, n. pag.

[11] "The anatomy of an enterprise social cyber attack, The Zero FOX Platform", USA. 2013.

[12] Miguel Ángel Justo (2013), "Delitos informáticos: la tecnología puesta al servicio del crimen", Web Oficial de Infojus Noticias. Fecha de consulta 12 de agosto de 2015 URL:http://infojusnoticias.gov.ar/nacionales/delitos-informaticos-la-tecnologia-puesta-al-servicio-del-crimen-2010.html

[13] Camilo Pérez García (2013), "Espionaje industrial: una realidad incómoda", Web Oficial de Colombia Digital. Fecha de consulta 12 de agosto de 2015 URL:http://colombiadigital.net/actualidad/articulos-informativos/item/4852-espionaje-industrial-una-realidad-incomoda.html

[14] "The risk of social engineering on information security: a survey of it professionals", California, USA. 2011.

[15] "Underestimating social engineering in it security governance", Web Oficial de Consultia. Fecha de consulta 12 de agosto de 2015 URL: http://www.consultia.co/underestimating-social-engineering-in-it-security-governance/

[16] Devin Luco, "The Art of Social Engineering", Seattle, USA. ASA Risk Consultants, 2013.

[17] Olavsrud, Thor (2010). "9 Best Defenses AgainstSocial Engineering Attacks." Web Oficial de eSecurity Planet. Oct 2010. Fecha de consulta 12 de agosto de 2015 URL: http://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-AgainstSocial-Engineering-Attacks.htm

[18] Olavsrud, Thor (2010). "9 Best Defenses AgainstSocial Engineering Attacks." Web Oficial de eSecurity Planet. Oct 2010. Fecha de consulta 12 de agosto de 2015 URL: http://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-AgainstSocial-Engineering-Attacks.htm

[19] IT Business Edge (2012). "Five Ways to Protect Your Organization Against Social Engineering." Web Oficial IT Business Edge. 2012. Web. 6 Apr 2013.Fecha de consulta 12 de agosto de 2015 URL: http://www.itbusinessedge.com/slideshows/show.aspx?c=81193.

[20] "The risk of social engineering on information security: a survey of it professionals", California, USA. 2011.

[21] Jared, Kee "Social Engineering: Manipulating the Source", SANS Institute InfoSec Reading Room, USA. 2008.

[22] Kenneth C. Laudan, Carol Guercio Traver, "Caso Sony, pagina 278", "E-Commerce", NY, USA. New York University. 2013.

[23] Digger For Truth (2013) "10 Reasons why I feel the Hare Krishnas are a Cult" Web Oficial: https://diggerfortruth.wordpress.com/2013/03/16/10-reasons-why-i-feel-the-hare-krishnas-are-a-cult. Fecha de consulta 1 de Diciembre de 2015, URL:

[24] Robert Cialdini, "YES, 50 ways to persuade people", Pag. 27. USA Cialdini 2009.

[25] John Leyden (2003) "Users Give away passwords for a cheap pen". Web Oficial del Diario Online The Register. Fecha de consulta 07 de Diciembre de 2015, URL: http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/

[26] Pau Navarro (2012"Herramientas de Persuación y Escasez". Web Oficial egolandseduccion.com. Fecha de consulta 07 de Diciembre de 2015, URL: http://www.egolandseduccion.com/herramienta-de-influencia-y-persuasion-escasez/

[27] Steffen Sorrell (2015) "The Internet of Things". URL: http://www.juniperresearch.com/researchstore/key-vertical-markets/internet-of-things/consumer-industrial-public-services.

[28] Marcus Nohlberg (2008) "Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks", Stockholm, Suecia. Stockholm University.

[29] Markus Huber, Stewart Kowalski, Marcus Nohlberg and Simon Tjoa,"Towards Automating Social Engineering Using Social Networking Sites", AT-1040 Vienna, Austria 2009.

[30] Tobias Lauinger, Veikko Pankakoski, Davide Balzarotti, Engin Kirda. Honeybot, Your Man in the Middle for Automated Social Engineering. EURECOM, Sophia-Antipolis, France, 2010

[31] NBC News (2005). Auditors Find IRS Workers Prone to Hackers. Web oficial de Noticias NBC, Fecha de consulta 29 de Diciembre de 2015 URL: http://www.nbcnews.com/id/7213173/ns/business-personal_finance/t/auditors-find-irs-workers-prone-hackers/#.VoNVoLbhBdg,

[32] Estadísticas de objetivos de phishing, por sitio web de estadísticas Stadisticas y Estudios (2015), Web Oficial de The Statistic Portal, Fecha de consulta 30 de Diciembre de 2015, URL: http://www.statista.com/statistics/266156/number-of-brands-hijacked-by-phishing-attacks.

[33] Steve Stasiukonis, Social Engineering, the USB Way (2006). Web Oficial Dark Reading Web Bussiness, Fecha de consulta 30 de diciembre de 2015 URL: http://web.archive.org/web/20060713134051/http://www.darkreading.com/document.asp?doc_id=95556&WT.svl=column1_1

Mauricio Castro: Realizó estudios de Gerencia Informática en la Universidad Dr. José Matías Delgado del 2002-2006. Graduado de Lic. En Admón. De Empresas con Énfasis en Computación de la Universidad Tecnológica de El Salvador (UTEC) en 2013. Actualmente cursa estudios de Maestría en Seguridad y Gestión de Riesgos Informáticos en la Universidad don Bosco (UDB). Posee dos certificaciones Microsoft MCP y MCDST y sus intereses de investigación incluyen la Ingeniería Social y gestión de riesgos y respaldo de datos. Actualmente es el encargado de elaborar boletines informativos y educacionales para el programa de educación a usuarios en LaGeo en temas de seguridad, en donde trabaja a tiempo completo en el área de seguridad de la información.