ISSN: 1692-7257 - Volumen 2 – Número 32 - 2018

Revista Colombiana de
Tecnologías de Avanzada

Recibido: 2 de abril de 2018
aceptado: 10 de junio de 2018

INGENIERÍA SOCIAL EN INSTITUCIONES DE EDUCACIÓN SUPERIOR

SOCIAL ENGINEERING IN HIGHER EDUCATION INSTITUTIONS

Esp. Santiago Acosta Pineda, Ph.D. John A. Bohada, MSc. Magda Lorena Pineda

Fundación Universitaria Juan de Castellanos, Facultad Ingeniería y Ciencias Básicas,
Grupo de Investigación MUISCA.
Tunja, Boyacá, Colombia.
Tel. (057) 3214759837.
E-mail: {jbohada, mlpineda}@jdc.edu.co.

Resumen: La Ingeniería Social hace referencia al conjunto de actividades que tienen como objetivo la manipulación de los seres humanos por medio de engaños con el único fin de obtener un acceso privado o información confidencial de las mismas personas, empresas o para nuestro caso, Instituciones de Educación Superior. Los practicantes de la Ingeniería Social se basan, en muchos casos, en el descuido, falta de conocimiento o incluso de la propia necesidad humana de comunicarnos, para captar datos e información que les permita realizar actividades fraudulentas en beneficio propio o incluso de una "comunidad". La Instituciones de Educación Superior, no son ajenas a estos ataques, incluso dado su grado de vulnerabilidad son propensas sin saberlo a perder toda su información y por ende poner en riesgo su continuidad. Por ello, el objetivo central de este artículo es hacer un estudio sobre la Ingeniería Social y sus antecedentes, las vulnerabilidades que poseen las Instituciones de Educación Superior y que pueden ser objeto de ataque, y en ese sentido, que estrategias se pueden proponer en favor de la protección de la información, así como recomendaciones generales y significativas para combatir la desinformación en este tema.

Palabras clave: Ingeniería Social, Delitos Informáticos, Seguridad Informática y de la Información, Seguridad en Instituciones de Educación Superior.

Abstract: Social Engineering refers to the set of activities that aim to manipulate human beings through deception with the sole purpose of obtaining private access or confidential information from the same people, companies or for our case, Higher Education Institutions. Practitioners of Social Engineering are based, in many cases, on the carelessness, lack of knowledge or even of the human need to communicate, to collect data and information that allows them to carry out fraudulent activities for their own benefit or even of a "community ". The Institutions of Higher Education are not immune to these attacks, even given their degree of vulnerability they are prone without knowing it to lose all their information and therefore put their continuity at risk. Therefore, the main objective of this article is to make a study about Social Engineering and its antecedents, the vulnerabilities that Higher Education Institutions have and that can be attacked, and in that sense, what strategies can be proposed in favour of the protection of information, as well as general and significant recommendations to combat misinformation in this area.

Keywords: Social Engineering, Computer Crimes, Information and Information Security, Security in Higher Education Institutions.

1. INTRODUCCIÓN

La Ingeniería Social la podemos definir como las diferentes formas, métodos o técnicas para engañar a las personas a realizar algo que ellas no desean conscientemente o en dado caso a publicar información confidencial o privada e incluso, hasta llegar a proporcionar un acceso privilegiado (Shimonski y Zenir, 2016). La Ingeniera Social no es catalogada como una Ciencia o Estudio Concreto, sino más bien se aprende en el ejercicio y practica de casos ya vistos, tanto de éxito como de fracaso en la aplicación de estos. El avance que ha tenido la Ingeniería Social se ha dado por la aplicación de los conocimientos en computación y el uso de Sistemas Informáticos, que hoy en día se ha masificado, los cuales, con las diferentes formas de engaño, convergen dando resultados nefastos a quien se le aplique un ataque de este tipo. Para las personas que utilizan la Ingeniería social, la recopilación de información, y en efecto existen muchas fuentes desde las cuales se podría recopilarla, es fundamental para sus propósitos, esto unido en muchos casos por el desconocimiento, desinterés o falta de prevención por parte de quienes poseen dicha información, de la importancia que tiene para el funcionamiento de una organización. Dentro de las fuentes de información susceptibles a ser utilizadas en ataques de Ingeniería social, tenemos: en primer lugar, el sitio web de la víctima, este punto para un Ingeniero Social es prioritario ya que lo orienta y ubica dentro del campo de acción de la víctima y posiblemente en muchas de sus falencias (Hadnagy, 2011), en segundo lugar, muchos Ingenieros Sociales toman como herramienta para encontrar información motores de búsqueda, pero el más utilizado es Google, por su masiva utilización, y en tercer lugar, la instrucción ***whois,*** una petición a la base de datos de donde se pueden sustraer datos y detalles vitales de la víctima, dichas bases de datos están alojadas en servidores y normalmente públicos, desde donde se evidencian la mayoría de Ataques Informáticos ya que son las puertas virtuales de toda entidad (United States Congress, 2001). Así mismo, podríamos nombrar los Medios Sociales como una de las recientes e importantes fuentes de recopilación de información ya que son un auténtico bum, donde se coloca todo tipo de información y que, en muchos casos, no se mide las consecuencias de tal situación. Como se puede deducir, con estas fuentes iniciales de información, ya se podría estar planeando, aplicando y concretando un ataque de Ingeniería Social a cualquier usuario y más en las Instituciones de Educación en donde, en la mayoría de los casos, no prevén o no tienen políticas concernientes a frenar dichos ataques. Por tanto, dichas Instituciones de Educación tienen muchas vulnerabilidades y están expuestas a ataques de ingeniería social, dejando a disposición de atacantes su activo más importante, la Información (Herrera, 2014; Medina, 2015).

En este sentido, este artículo pretender dar a conocer en que consiste la Ingeniería Social, el grado de vulnerabilidad a las que están expuestas las Instituciones de Educación Superior y que estrategias se podrían seguir para no ser víctimas de esta creciente forma de delito, para así lograr reducir el grado de desinformación que existe respecto a este tema.

2. METODOLOGÍA

Para el desarrollo de la presente investigación, en primer lugar, se hizo una búsqueda bibliográfica que permitiese describir la situación actual de la Ingeniería Social, particularmente en las Instituciones de educación Superior. En segundo Lugar, se hizo una investigación en varias Instituciones de Educación Superior[1]. Para tal efecto, se tomaron las principales formas para realizar Ingeniería Social y se aplicaron a las diferentes instituciones, dando a conocer los resultados obtenidos. Finalmente, tomando como base los resultados obtenidos, se proponen estrategias que permitan contrarrestar dichas vulnerabilidades.

3. RESULTADOS

3.1 Ingeniería Social

La Ingeniería Social, cuyo nombre se confunde con algo positivo, no es nada más que la forma de hackear a seres humanos, siendo éste un método de ataque no convencional que se fundamenta en la manipulación de las personas por medio de estrategias de engaño con el único fin de obtener un acceso privado o información confidencial para ser utilizada en actividades fraudulentas y que ocasionan daño a dichas personas o instituciones. En este sentido, se han desarrollado diferentes técnicas que pueden ser clasificadas según el recurso que desean atacar, por lo tanto, podemos decir que existen técnicas de Ingeniería Social basada en computadores y técnicas de Ingeniería Social basada en el recurso humano (Bermúdez, 2015). Respecto a las técnicas basadas en computador, éstas se caracterizan por hacer uso exclusivo de herramientas informáticas para la realización de los ataques, entre ellas podemos indicar las siguientes: Phising o envio de correos falsos los cuales invitan al usuario a registrarse en web fraudulentas para obtener información privada o también incorporan archivos maliciosos o malware que tienen el mismo objeto; Spam o correo no deseado, que en muchos casos buscan colapsar servidores o los correos de usuario y con ello, intentar hacer ataques de pishing; Pop-up’s, o ventanas

[1] El nombre de las Instituciones y su localización se mantienen en reserva por razones de seguridad y confidencialidad

emergentes las cuales son utilizadas por los que practican la Ingeniería Social para introducir códigos maliciosos.

Respecto a las técnicas basadas en el recurso humano, éstas han sido la que mayor trascendencia han tenido dentro de la Ingeniería Social, y se basan en aprovechar las características intrínsecas que como humanos tenemos: curiosidad, deseo, codicia, miedo incluso la bondad, las cuales son estudiadas con el fin de obtener fraudulentamente información (Landwehr y Landwehr-Sigg, 2014). En este sentido, podemos indicar las siguientes técnicas basadas en el recurso humano: Suplantación de identidad (Pacheco y Jara, 2009), Espiar por encima del hombro (Watson Gavin, 2014), Buscar en la basura (Olmus. (2015), Ingeniería Social Inversa (Jaramillo, 2010), Desarrollar Confianza (Thomas, 2014), Afectividad (Ian, 2008), Sobrecarga (Moutona, et al., 2016), Reciprocidad (Mitnick, et al., 2011), Relaciones basadas en Engaños (Giboneya, 2016) y Escuchar detrás de las Puertas (Revista Semana, 2010), todas ellas aplicadas para fines fraudulentos.

La forma de engaño basada en el recurso humano ha crecido tanto que con el paso de los años muchas instituciones no solamente centran su necesidad de seguridad en la parte física, sino que también, en el recurso humano dando capacitaciones constantes, pruebas de seguridad y aplicando herramientas preventivas y correctivas. Desafortunadamente, esto no es la constante y actualmente muchas Instituciones de Educación Superior en el mundo han sido la plataforma de despegue de grandes ciber ataques (Santiago, 2016), algunos de ellos son los que se presentan en la siguiente sección.

3.2 Ataques de Ingeniería Social a Instituciones de Educación Superior

La Ingeniería Social, como se ha mencionado anteriormente, afecta la integridad de la información, lo cual lo demuestran diversos estudios realizados en la última década. Dichos estudios han evidenciado que el en un alto porcentaje, cerca del 50%, de las Instituciones que hicieron parte de dicho estudio indicaron haber sido víctimas (Check Point, 2011; Masana, 2002), además, que un alto porcentaje de las instituciones atacadas toma la decisión de no hacer ningún tipo de denuncia, lo cual impide o hace difícil conocer la magnitud de los ataques realizados y el grado de afectación que dichas instituciones han tenido. En este sentido, la Universidad de Carnegie Mellon (Westby, 2012) efectúo un estudio a diversas instituciones para poder determinar los tipos de ataque de Ingeniería Social que habían sufrido, dando como resultado que la personificación y/o suplantación de la identidad, con un 66%, el pishing con un 15%, han sido las técnicas mayormente utilizada para el robo de información vital de las instituciones objeto del estudio (Bassett, 2015). En el año 2012 se hizo público el ataque a más de 50 universidades de los EE. UU, las cuales fueron víctimas de un grupo de "hackers" llamado GhostShel, los cuales filtraron información como "nombre, correo electrónico, contraseña, dirección postal y teléfono de más de 120.000 estudiantes y miembros administrativos de dichas Instituciones (B:Secure, 2012; United States Congress, 2009). Otros ejemplos de ataques recibidos es el ocurrido en la Universidad de Carolina del sur (Álvarez, 2012), la cual perdió 34.000 registros con información personal, .en 2013 la Universidad de Stanford fue afectada de la misma forma donde personal no autorizado sustrajo datos confidenciales de los integrantes de la institución (B:Secure, 2013) y recientemente, en 2017, un estudiante de la Universidad de Iowa, fue acusado de secuestrar las cuentas de varios de sus profesores para cambiar las notas y obtener, fraudulentamente exámenes (Muñoz, 2017.).

En América Latina, este fenómeno no es ajeno a sus Instituciones de Educación Superior, por ejemplo, en Chile se reportó que piratas informáticos atacaron el sitio web de La Pontifica Universidad Católica de Chile, alojando sitios web de pornografía (La Tercera, 2012), en Brasil en el 2015 dos portales de la Universidad Federal de Río de Janeiro (UFRJ) fueron atacados por un grupo de piratas informáticos, presuntamente yihadistas, que publicaron mensajes de protesta por el "irrespeto al profeta Mahoma" y amenazas contra el Estado de Israel (Agencia EFE, 2015).

En instituciones de Colombia, diversos casos han sido denunciados y divulgados con la finalidad de generar estrategias de prevención. Ejemplo de ello podemos citar el ataque que afectó en el año 2008 a la Universidad Surcolombiana "USCO" (Informador, 2009), donde seis estudiantes adscritos a tres carreras profesionales de esa Institución, accedieron a los sistemas de información y modificaron 366 calificaciones, aprovechando el periodo de vacaciones del claustro, y lo más agravante es que todo se ejecutó desde un café internet de la zona y con herramientas muy básicas, nada sofisticadas, situación que indica esos estudiantes ya contaban con información suficiente para poder acceder al sistema, aspecto fundamental para un ataque de Ingeniería social, y el grado de vulnerabilidad que tienen. Igual situación ocurrió en el año 2015 (El Espectador, 2015), donde fue sustraída la información de las cuentas de correo electrónico de los candidatos a la rectoría de la Universidad Nacional de Colombia, desde los cuales, además, enviaron mensajes no agradables a los estudiantes.

Teniendo en cuenta los antecedentes descritos anteriormente podemos aseverar que la frecuencia de ataques de Ingeniería Social a Instituciones de Educación Superior es bastante grande, sin embargo, no hay divulgación de estos por el hecho que a dichas

Instituciones por conveniencia, no hacen público dichas situaciones, además, no quieren que se sepa la gran vulnerabilidad que poseen. Dicha situación se presenta a la gran cantidad de usuarios que se conectan a sus redes, que visitan sus páginas web y sus redes sociales (Arévalo, 2015), el recurso humano que a diario realiza conexiones laborales desde lugares fuera de sus instalaciones y más aún la falta de capacitación y concientización en temas nuevos sobre Seguridad Informática, su prevención y corrección y de los peligros que entrañan técnicas enfocadas al engaño como lo es la Ingeniería Social (Wark, 2004).

3.3 Estudio de Vulnerabilidades en Instituciones de Educación Superior

Para tener un mejor grado de conocimiento sobre las vulnerabilidades a las que están expuestas las Instituciones de Educación Superior respecto a la Ingeniería Social, se hizo un estudio a cinco (5) Instituciones de Educación Superior, a las cuales se les aplicó las diferentes técnicas descritas en la Tabla 1 y los resultados obtenidos son los que se plasman en la Tabla 2.

Tabla 2. Estudio de vulnerabilidades en Instituciones de educación Superior

Técnica	Resultados del estudio
Suplantación de identidad	En todas las instituciones se evidenció que la suplantación como estudiante de la institución es viable, de igual forma, en épocas de inscripciones y matrículas, hay acceso libre a las instituciones, donde puede ingresar cualquier persona que muestre algún interés por cualquier programa ofertado. Así mismo, se evidenció que, en tres de las cinco instituciones, no se verifica que el portador del carnet sea quien dice ser, lo cual hace posible el préstamo de este documento e ingresar sin ningún problema. En una institución donde se desarrollaba un acto académico, el solo hecho de portar una escarapela dio la posibilidad de ingreso y, por ende, la posibilidad de acceso a información y de quienes participaron en dicho evento. Una vez obtenido el acceso a la institución, se pudo desarrollar varias técnicas de ingeniería social, descritas en este documento.
Espiar por encima del hombro	En tres de las cinco instituciones se evidenció que no hay seguridad en la documentación de las dependencias, son comunes encontrarlos encima de los escritorios sin ningún tipo de protección al público en general, incluso, información digital está expuesta y a la mano de quien se encuentre en dichas dependencias. Por otro lado, en todas las instituciones se evidenció que, en cafeterías, grupos de estudio, bibliotecas, etc., los estudiantes no toman ningún tipo de prevención respecto a los accesos que hacen a los diferentes sistemas de información, correos o grupos sociales.
Buscar en la basura	En cuatro Instituciones no cuentan con procedimientos para el control de los documentos que "ya no necesitan", en la institución restante, tienen un procedimiento y área de triturado de papel, sin embargo, no hay control ni seguridad en dicha dependencia. En una revisión usando esta técnica, se pudieron encontrar documentos como facturas, calificaciones, notas, desprendibles de pago, UBS, DVD, incluso carnets estudiantiles para renovar o dañados, los cuales pueden permitir una suplantación de identidad fácilmente.
Ingeniería Social Inversa	Esta técnica no se ejecutó en todas las instituciones, pero sí por medio de un típico caso de aprovechamiento de confianza, en tres instituciones se logró obtener la ubicación de los equipos de cómputo, de los centros de datos y que sistemas de información utilizaban. Así mismo, se detectó una vulnerabilidad en algunas oficinas dado que los funcionarios de esas dependencias dan la espalda al usuario que llega solicitar un servicio, lo cual permite que el equipo de cómputo pueda ser desconectado sin conocimiento del funcionario y luego, la persona interesada en hacer el fraude, brindar su servicio para su reconexión, permitiendo que en algún descuido puedan sustraer la información de dicho dispositivo.
Desarrollar Confianza, afectividad, sobrecarga y reciprocidad	Para obtener resultados de esta técnica, se hicieron dos pruebas, la primera consistía en hacer llamadas telefónicas con la dependencia de la recepción, donde se evidenció en todas las instituciones la falta de capacitación en seguridad, donde de igual forma, se obtuvo información relevante de la Institución. En segundo lugar, se informó al área de seguridad de la institución sobre una supuesta pérdida de un objeto personal, en dos Instituciones accedieron a abrir los locker's para revisar si se encontraba o no dicho objeto, lo cual evidenció que, la seguridad de éstos es claramente vulnerable y que no existen protocolos para este fin. También se detectó que, en dos Instituciones, el personal de servicios tiene acceso a casi todas las dependencias, lo cual genera una mayor vulnerabilidad, y que con técnicas de confianza, afectividad y sobrecarga aplicadas a dicho personal, se pueda acceder a dichas dependencias. Así mismo, en los procesos de inducción de estudiantes nuevos, estos son llevados a diferentes dependencias para que conozcan su

	funcionamiento, situación que, dado el afán de protagonismo de muchos funcionarios, llevan a que brinden información más allá de la solicitada.
Escuchar detrás de las Puertas	En todas las instituciones se pudo evidenciar que el acceso a las salas de reuniones no es restringido, lo cual lleva a que se puedan escuchar decisiones que puedan ser tomadas al interior de estas, igual ocurre con muchas dependencias. Las cafeterías son una fuente inagotable para la aplicación de esta técnica, allí se reúnen estudiantes, docentes, administrativos e incluso directivos y comentan situaciones o decisiones que pueden ser tenidas en cuenta para un ataque de Ingeniería Social.

Como se puede evidenciar en este estudio, la suplantación de identidad es la técnica que, en estos casos, brindó la posibilidad o dio la puerta de entrada para la aplicación de las demás técnicas de Ingeniería Social. La falta de conocimiento y poca capacitación del personal que labora en dichas Instituciones, hacen que sean vulnerables a cualquier ataque.

3.4 Estrategias de Prevención y corrección de Ataques de Ingeniería Social para las Instituciones de Educación Superior.

Como se ha podido observar, el recurso humano, desafortunadamente, es el eslabón más débil en las Instituciones de Educación Superior, para vulnerar y generar ataques de Ingeniería Social. En este sentido, pueden existir muchas estrategias que permiten prevenir dichos ataques y, por ende, salvaguardar la información vital de las Instituciones. Por tanto, a continuación, se presentan algunas recomendaciones basadas en estudios previos (Arbeláez, 2013; Sandoval, 2011) y en los resultados obtenidos del estudio realizado a las Instituciones:

a) **Desarrollo e implementación de Políticas y planes de Seguridad**. Es de vital importancia que cada institución haga un proceso de autoevaluación y determine el grado de vulnerabilidad que tienen frente a los delitos informáticos y en especial, a la Ingeniería social basada en el recurso humano. Tomando como base dichos resultados y teniendo en cuenta que la información debe ser confidencial, íntegra y disponible, deben desarrollar políticas y planes de seguridad que les permita salvaguardar la información. Un referente importante para la construcción de estas políticas es el desarrollado por el Gobierno Nacional de Colombia en su versión 07-2017 (Presidencia de la República, 2017).

b) **Capacitación**. Las instituciones deben tomar muy en serio el tema de seguridad y más, la Ingeniería Social, por ello, la estrategia más importante concierne a la programación de planes de capacitación a todo el personal, a todos los niveles (estudiantes, docentes, administrativos y directivos) y según el rol que desempeñen frente a la información, donde se expliquen todas sus técnicas, y el cómo deben actuar frente a personas que quieren hacer un ataque de Ingeniería Social. El riesgo de suplantación de identidad debe reducirse o eliminarse y desarrollar políticas de seguridad que apunten a la prevención de esta técnica. El conocimiento de este tipo de fraudes hace que sea cada vez más difícil obtener información de forma fraudulenta, minimizando así muchas de las técnicas descritas en este artículo.

Unido a las dos estrategias anteriores, es importante evaluar que la Ingeniería Social también tiene técnicas basadas en el uso de computador como herramienta para hacer ataques, por ello se recomiendan las siguientes estrategias:

a) **Backup´s o Copias de Seguridad**: La obtención, cambio o eliminación de información como calificaciones, es una práctica habitual de la Ingeniería social en las Instituciones, por tanto, implementar políticas de respaldo de la información ayudará a minimizar este riego. No olvidar que dicha información debe estar protegida tanto física como lógicamente para evitar accesos no autorizados a la misma.

b) **Autenticación**: Se recomienda que el logueo a las plataformas, sistemas, aplicaciones y demás, debe controlarse y determinar que cada usuario cree cuentas separadas, contraseñas distintas y fuertes, teniendo en cuenta las indicaciones que nos proveen las guías internacionales de seguridad y de la Información. Para tal fin, cada Institución deberá crear políticas de seguridad relacionados con las claves de acceso.

c) **Monitoreo**: Se recomienda el uso de programas informáticos tales como Sniffer o Sistemas de Detección de Intrusos (IDS por sus siglas en inglés) que permiten monitorear computadores o una red en tiempo real, permitiendo de esta forma detectar y minimizar los riesgos de accesos no autorizados a la información.

d) **Almacenamiento en la nube:** Esta nueva tendencia donde el almacenamiento de la información no se hace directamente en dispositivos físicos de las Instituciones, sino que se valen de servicios que en este sentido prestan otras organizaciones y cuyo acceso solamente se hace por Internet, puede ser una estrategia interesante. Por tanto, la decisión de tomar esta estrategia debe salir de una evaluación minuciosa donde se los riesgos, costos, acceso y disponibilidad de la información son mejores frente a la solución tradicional.

e) **Actualización periódica de dispositivos.** Para que todo lo anterior tenga éxito, es importante que todos los dispositivos que hacen parte de la seguridad de la información (sistemas operativos, antivirus, etc.), sean evaluados periódicamente y tengan las últimas actualizaciones en cuanto a seguridad se refieren. De nada sirve tener planes de seguridad, capacitaciones y buenas estrategias de seguridad, si los dispositivos electrónicos en los cuales se soporta y almacena la información son obsoletos y están totalmente desactualizados.

Finalmente, es importante conocer algunas estrategias que permitan dar respuesta a los incidentes que se presenten frente a un ataque de Ingeniería Social (OCDE, 2004; Lockhart, A. 2007; Bathurst, 2013; Broad y Bindner, 2014; Myatt, 2014; Wimmer, 2015; Krombholz, 2015; Gevers, 2016; Segal, 2016, Alvernia, 2017).

a) **Conformación de un equipo de respuesta a incidentes**. Este equipo está constituido por personas que cuentan con experiencia y la formación necesaria para poder actuar frente a incidencias y desastres que pudieran afectar la integridad, confidencialidad y disponibilidad de la información. Además, serán responsables del seguimiento en el cumplimiento de las políticas y planes de seguridad adoptados por la institución.
b) **Definición de una guía de procedimientos.** Basado en las políticas y planes de seguridad, se debe desarrollar procedimientos o pasos concretos para la recuperación rápida y eficiente en caso de un incidente, a fin de salvar los datos y la continuidad de los sistemas afectados.
c) **Detección de un incidente de seguridad.** La institución debe estar en constante revisión de los sistemas de información (sistemas administrativos, sistemas académicos servicios) y comunicación (redes y accesos) en busca de cambios o irregularidades que den pistas de una posible intrusión.
d) **Análisis del Incidente.** Si lo anterior ha fallado y se presenta un posible ataque**,** se debe investigar sobre el alcance del incidente, cuáles fueron sus causas, que personas, equipos, sistemas o servicios se pudieron ver involucrados y/o afectados y cuáles fueron sus consecuencias.
e) **Contención, Erradicación y Recuperación**. Esta estrategia se hace una vez se haya hecho el análisis del incidente que afectó a la institución, donde cada una de las tres actividades representan momentos distintos después de ejecutado un ataque. La contención busca determinar cómo limitar el accionar del incidente mientras se establece su origen, se debe tener cuidado puesto cualquier acción a desarrollar puede ocasionar daños mayores al sistema afectado. En la erradicación se ejecutan todas las tareas necesarias para eliminar la causa del incidente, y en la recuperación se enfoca a recobrar la funcionalidad de los sistemas afectados y el retorno de la operatividad segura de los mismos.
f) **Identificación del atacante y posibles actuaciones legales**. En caso de lograr identificar el atacante, la Institución debe contar con una política que indique cuales son los mecanismos legales para actuar frente a esta situación. En muchos casos, esta actividad es inherente al actuar de los reglamentos internos de la Institución.
g) **Comunicación con terceros y relaciones públicas**. Se debe contemplar, además, el actuar que debe hacer la institución frente a terceros que se vieron afectados con el incidente (personal interno y externo de la institución), los mecanismos de comunicación de las causas y consecuencias del incidente y el que hará la institución frente a dicha situación.
h) **Documentación del incidente de seguridad**. Es importante una vez ocurrido el incidente, que la institución mediante su equipo de respuesta registre la totalidad del ataque para que sirva de base documental para futuras actuaciones, en tales casos, se debe registrar datos como: la descripción del incidente, los hechos, daños producidos en los sistemas, las actuaciones por parte de la Institución, listar las evidencias y recomendaciones, etc.
i) **Análisis y revisión a posteriori del incidente**. Una vez registrado el incidente, es necesario hacer una retroalimentación con el fin de avaluar lo aprendido por parte de la Institución y hacerlo parte de los planes de capacitación que para tal fin se proponga. En este sentido, cabría el hecho que, si se conoce el incidente, el grado de ocurrencia de este en el futuro sería mínimo.

4. DISCUSIÓN

Tener en cuenta que el activo más valioso de cualquier Institución es su información, y, por tanto, protegerla debe ser una de sus principales prioridades. La información bien protegida garantizará su continuidad en el tiempo. En la última década, se ha incrementado el uso de diferentes técnicas o herramientas que buscan por cualquier medio vulnerar los sistemas de seguridad para obtener información confidencial para usarla con fines diferentes a su objeto, incluso para causar daño o entorpecer el funcionamiento de una determinada Institución. En este sentido, técnicas basadas en la Ingeniería Social han tomado fuerza en los últimos años, donde basados en el engaño, buscan vulnerar las debilidades que como humanos tenemos para obtener dicha información confidencial. Por ello y como se pudo evidenciar en este artículo, una de las mayores debilidades que tienen las Instituciones de Educación Superior frente ataques de ingeniería social, es precisamente este recurso el cual es el más atacado, por tanto, la adopción de políticas de

seguridad y/o planes de seguridad para combatir esta situación es urgente y no aplazable para minimizar los fraudes fruto de la manipulación que puedan hacer al personal de una Institución. De igual forma, el conocimiento que se tenga frente a la Ingeniería social ayuda a minimizar los ataques que se puedan hacer, es así que, la capacitación a todo el personal de la Institución frente a este tema es fundamental y debe estar integrado en las políticas y planes de seguridad adoptados por cada Institución.

En todas las instituciones objeto de estudio de este artículo, se constató que tienen una unidad o dependencia encargada de la gestión de los servicios tecnológicos, sin embargo, su orientación está hacia la seguridad se basa en el componente físico y lógico, desconociendo la importancia que tiene el recurso humano como "objeto" fácilmente vulnerable y que puede ser la puerta de entrada para un ataque a la información de la Institución. Tal es el caso que el personal de servicios generales de las cinco Instituciones analizadas tiene acceso a todas las dependencias de su institución y, aún, nunca son tenidos en cuenta en procesos de seguridad, los cuales los hace muy atractivos para un practicante de ingeniería social. Situación similar ocurre con estudiantes e incluso docentes, por tanto, es importante tomar conciencia de la importancia del recurso humano frente a la confidencialidad, integridad y disponibilidad de la información en una Institución.

5. CONCLUSIONES

La Ingeniería social basa su éxito en la manipulación psicológica de los valores de las personas que, unido a su desconocimiento respecto a este tipo de fraude, hacen que sean muy vulnerables y ofrezcan voluntariamente información confidencial de una Institución. Además, muchos de los casos de fraude por este medio quedan impunes por que las personas afectadas, por temor al qué dirán, no comunican o no cuentan dicha situación contribuyendo de esta forma a que se den más ataques similares.

Según el estudio presentado en este artículo, la suplantación de identidad ha sido la técnica puerta de entrada a ataques de ingeniería social en las Instituciones de Educación Superior, Por tanto, el tomar medidas para minimizar esta falencia contribuirá a contrarrestar este tipo de ataques.

El desarrollo de políticas y planes de protección de la información, unido con procesos continuos de capacitación ayudarán a mejorar la confidencialidad, integridad y disponibilidad de la información de las Instituciones de Educación Superior.

Tener en cuenta siempre que el recurso humano es un factor muy importante en el proceso de seguridad de la información, todos los funcionarios juegan un papel primordial en la continuidad del objeto de las Instituciones. El desconocer esta situación, será el eslabón débil sobre el cual se harán los ataques de la Ingeniería Social.

6. REFERENCIAS

Álvarez, Ángel. (2012). Hackean la Universidad de Carolina del Sur, roban datos de 34,000. b:SECURE. http://www.bsecure.com.mx/featured/hackean-la-universidad-de- carolina-del-sur-roban-datos-de-34000/

Agencia EFE. (2015). Supuestos yihadistas piratean dos portales de una universidad brasileña. http://www.caracol.com.co/noticias/internacionales/supuestos-yihadistas-piratean-dos-portales-de-una-universidad-brasilena/16173/nota/2591949.aspx

Alvernia, Sergio y Rico, Dewar. (2017). Análisis de una red en un entorno IPV6: una mirada desde las intrusiones de red y el modelo TCP/IP, Revista Colombiana de Tecnologías de Avanzada (RCTA), Universidad de Pamplona (Colombia), Vol.1, 29.

Arbeláez, Ana. (2013). Ingeniería Social: El Hackeo Silencioso. http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/

Arévalo, José G., et al. (2015). Redes sociales digitales: una aproximación a los riesgos en sistemas de información gerencial. Revista Colombiana de Tecnologías de Avanzada (RCTA), Universidad de Pamplona (Colombia), Vol. 1, 25

Bathurst, R. (2013). The hacker's guide to OS X: exploiting OS X from the root up. Waltham, Mass.: Syngress. http://resolver.library.cornell.edu/cgi-bin/EBookresolver?set=Books24x7&id=47323

Bassett, G. (2015). Database Breach Investigations Report, Verizon. https://securityblog.verizonenterprise.com/

B:Secure. (2012). Hackers filtran datos de Harvard, Stanford y Princeton". http://www.bsecure.com.mx/featured/hackers-filtran-datos-de-harvard-stanford-y-princeton/ Stanford

B:Secure. (2013). Hackean a la Universidad de para hurtar datos de su sistema.

http://www.bsecure.com.mx/featured/hackean-a-la-universidad-de-stanford-para- hurtar-datos-de-su-sistema/

Bermúdez Penagos, Edilberto. (2015). Ingeniería Social, un factor de riesgo informático inminente en la Universidad Cooperativa de Colombia. Tesis Especialización en Seguridad Informática, UNAD, Neiva.

Broad J., y Bindner, A. (2014). Hacking with Kali: practical penetration testing techniques. (First edition.). Waltham, MA: Syngress. http://proquest.safaribooksonline.com/9780124077492

Check Point. (2011). A2Secure, Informe de Seguridad, 22. http://www.a2secure.com/empresa/noticias-seguridad/269-48-de-las-empresas-blanco-de-ataques- de-ingenieria-social

El Espectador. (2015). Hackean cuentas de correo de candidatos a rectoría de la Universidad Nacional. http://www.elespectador.com/noticias/educacion/hackean- cuentas-de-correo-de-candidatos-rectoria-de-uni-articulo-549936

Gevers, I. (2016). Hacking habitat: art of control: art, technology and social change. Rotterdam: Nai010 Publishers.

Giboneya, Justin Scott, Gainer Proudfootb, Jeffrey, Goela, Sanjay y Valacichc, Joseph S. (2016). The Security Expertise Assessment Measure (SEAM): Developing a scale for hacker expertise, in Computers & Security, NY 12222, USA: CrossMark, 60. 37-51. http://www.sciencedirect.com/science/article/pii/S0167404816300323

Hadnagy, Christopher. (2011). Ingeniería Social el Arte del Hacking Personal, USA, Multimedia-Anaya Interactiva, 400, 39-41.

Herrera, Héctor. (2014). El Eslabón más débil de la cadena: factor humano. ActivosTI. http://www.activosti.com/el-eslabon-mas-debil-de-la-cadena-factor-humano/.

Ian, Man. (2008). Social Engineering, in Hacking the Human, England: Gower Publishing Limited, 1, 1-252. https://books.google.com.co/books?id=U1IihJpdrGwC&printsec=frontcover&dq=social+engineering&hl=es-419&sa=X&ved=0ahUKEwiu2JrD4cbPAhVKWx4KHRjDAnkQ6AEILjAC#v=onepage&q=social%20engineering&f=false

Informador. (2009). Estudiantes "hackean" calificaciones de su Universidad. http://www.informador.com.mx/internacional/2009/75916/6/estudiantes-hackean-calificaciones-de-su-universidad.htm

Jaramillo H., Lucia Gabriela. (2010). Estudio del grado de incidencia de la ingeniería social en la primera fase de los ataques informáticos que se realizan actualmente en las empresas privadas del ecuador, Trabajo de grado Ingeniero de Sistemas. Quito: Universidad Internacional SEK. Facultad de Ciencias y Telecomunicaciones.

Krombholz, Katharina, et al. (2015). ¿Qué es la ingeniería social? En qué consiste y cómo evitar. in Journal of Information Security and Applications. Vienna, Austria: SBA Research, 22, 113-122. http://www.sciencedirect.com/science/article/pii/S2214212614001343

La Tercera. (2012). Hackean página web de la Universidad Católica con sitios pornográficos. http://www.latercera.com/noticia/nacional/2012/03/680-437360-9-hackean-pagina-web-de-la-universidad-catolica-con-sitios-pornograficos.shtml

Landwehr, D. y Landwehr-Sigg, S. (2014). Hacking. [Basel]: Merian.

Lockhart, A. (2007). Network security hacks. (2nd ed.), Sebastopol, CA: O'Reilly.

Masana, S. (2002). El ciberterrorismo: ¿una amenaza mundial para la paz mundial?, Facultad Latinoamericana de Ciencias Sociales. http://www.argentina-rree.com/documentos/ciberterrorismo.pdf

Medina, Édgar. (2015). Ingeniería social, la razón del éxito de los ladrones digitales. Redacción Tecnósfera. http://www.eltiempo.com/tecnosfera/novedades-tecnologia/de-que-se-trata-la-ingenieria-social/16020156

Mitnick, K. D., Simon, W. L. y Wozniak, S. (2011). Ghost in the wires: my adventures as the world's most wanted hacker. New York: Little, Brown.

Moutona, Francois, Leenena, Louise y Venterb, H.S. (2016). Social engineering attack examples, templates and scenarios. in Computers & Security. Pretoria, South Africa, Elseiver. 59, 186-209. http://www.sciencedirect.com/science/article/pii/S0167404816300268

Muñoz, Cesar. (2017). Universitario fue arrestado por robar cuentas de profesores usando un keylogger. http://www.fayerwaver.com].

Myatt, M. (2014). Hacking leadership: the 11 gaps every business needs to close and the secrets to closing them quickly, Hoboken, N.J.: John Wiley & Sons. http://resolver.library.cornell.edu/cgi-bin/EBookresolver?set=Books24x7&id=62639

OCDE. (2004). Organisation for Economic Cooperation and Development. Directrices de la OCDE para la seguridad de sistemas y redes de información: hacia una cultura de seguridad. Paris: OECD. http://dx.doi.org/10.1787/9789264065819-es

Olmus. (2015). Buscando en la basura.Trashing. Nas/servicios/net. http://www.olmus.es/?p=1585

Pacheco G., Federico y Jara, Hector. (2009). Hackers al descubierto, entienda sus vulnerabilidades evite que lo sorprendan. in Users Manuales. https://books.google.com.co/books?id=q8j4UCoBQlkC&pg=PA24&dq=Fase+1:+Footprinting+(Reconocimiento)&hl=es-419&sa=X&ved=0ahUKEwi7w4mf0LzOAhWEOSYKHchbBOgQ6AEIGjAA#v=onepage&q=Fase%201%3A%20Footprinting%20(Reconocimiento)&f=false

Presidencia de la República. (2017). Manual de Políticas de Seguridad de la Información. Departamento Administrativo de la Presidencia. http://es.presidencia.gov.co/dapre/DocumentosSIGEPRE/M-TI-01-Manual-Politicas-Seguridad-Informacion.pdf

Revista Semana. (2010). Espías S.A. http://www.semana.com/economia/articulo/espias-sa/43741-3

Sandoval Castellanos, Edgar Jair. (2011). Defensa Digital e Ingeniería Social: Corrompiendo la mente humana. Revista Seguridad. 1(10). 23-25. http://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

Santiago, Enrique J. y Sánchez, Jesús. (2016). Diseño de un sistema multiagentes híbrido basado en aprendizaje profundo para la detección y contención de ciberataques, Revista Colombiana de Tecnologías de Avanzada (RCTA), Universidad de Pamplona (Colombia), Vol. 2, 28.

Segal, A. (2016). The hacked world order: how nations fight, trade, maneuver, and manipulate in the digital age. (First edition.), New York: PublicAffairs.

Shimonski, Robert y Zenir, John. (2016). Chapter 3-Social Engineering, in Cyber Reconnaissance, Surveillance and Defense, Ingeniería Social, USA: Edit. Allison Bishop. 1, 85-112. http://www.sciencedirect.com/science/article/pii/B9780128034057000060

Thomas, Valerie. (2014). Chapter 7 – Social Engineering, in Building an Information Security Awareness Program, VA, USA: Securicon, Lorton, 45-63. http://www.sciencedirect.com/science/article/pii/B9780124199675000077

United States Congress. (2001). WHOIS database: privacy and intellectual property issues: hearing before the Subcommittee on Courts, the Internet, and Intellectual Property of the Committee on the Judiciary, House of Representatives, One Hundred Seventh Congress, first session. Washington: U.S. G.P.O. http://purl.access.gpo.gov/GPO/LPS42925

United States Congress. (2009) Hacking the homeland: investigating cybersecurity vulnerabilities at the Department of Homeland Security: hearing before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology of the Committee on Homeland Security, House of Representatives, One Hundred Tenth Congress, first session. Washington: U.S. G.P.O.

Watson Gavin. (2014). Chapter 11 – The Physical Attack Vector, in Social Engineering Penetration Testing, Utah, USA: RandomStorm Limited. 255-270. http://www.sciencedirect.com/science/article/pii/B9780124201248000119

Wark, M. K. A. (2004). Hacker manifest. Cambridge, MA: Harvard University Press.

Westby, Jody R. (2012). How Boards & Senior Executives Are Managing Cyber Risks, Ed. Adjunct Distinguished Fellow, CyLab CEO, Global Cyber Risk LLC. http://www.google.es/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CCUQFjAA&url=http%3A%2F%2Fwww.hsgac.senate.gov%2Fdownload%2Fcarnegie-mellon-cylab-cybersecurity-report&ei=W9BYVbCUCs-wsASPnYGQDA&usg=AFQjCNHhCCeRNXeVo6Bi4U3iWYNg0Ldilg&bvm=bv.93564037%2Cd.cWcHow+

Boards+&+Senior+Executives+Are+Managing+Cyber+Risks

Wimmer, Bruce. (2015). Business Espionage, 5 ed., USA: Risk, Threats, and Countermeasures, 59-73. http://www.sciencedirect.com/science/article/pii/B9780124200548000005X