INGENIERÍA SOCIAL COMO DELITO INFORMÁTICO EN LAS GRANDES EMPRESAS COLOMBIANAS

ING. EDWIN ALBERTO NOVOA GUTIÉRREZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BELLO, ANTIOQUIA
2018

INGENIERÍA SOCIAL COMO DELITO INFORMÁTICO EN LAS GRANDES EMPRESAS COLOMBIANAS

ING. EDWIN ALBERTO NOVOA GUTIERREZ

Trabajo Monográfico
Presentado como requisito para optar el título
Especialista en Seguridad Informática

Ing. Edgar Alonso Bojaca Garavito
Director de Proyecto

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
FACULTAD DE INGENIERÍA Y CIENCIAS BÁSICAS
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BELLO, ANTIOQUIA
2018

Nota de Aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Bello, 12 de diciembre de 2018

DEDICATORIA

Al Creador que en la cotidianidad me permite experimentarme realmente vivo, a ver desde diversas perspectivas y desde las mismas aprender y desaprender para romper paradigmas y visualizar nuevos caminos de aprendizaje.

De manera muy especial dedico este trabajo a mi madre, Hilda Gutiérrez Landazábal, quien a lo largo de mi vida veló por mi bienestar y educación siendo mi apoyo en cada momento sin importar distancias; inició este proceso conmigo y hoy se encuentra gozando de la pascua junto al Creador.

AGRADECIMIENTOS

Al Creador que me ha posibilitado de perdurables capacidades, para alcanzar cada objetivo que me trazó con paciencia y perseverancia.

A mi familia, por su apoyo incondicional y aún en la distancia me animan cada día a continuar sin importar las adversidades.

A mí pareja que me brindó una voz de aliento para seguir adelante con este proyecto, gracias por sus consejos y entrega en los momentos que los necesité.

A mis compañeros de trabajo y de estudio, quienes han compartido sus conocimientos de manera desinteresada y me enseñan que solo con ahínco se alcanzan grandes cosas y se hacen inmensas transformaciones.

A los docentes e ingenieros Christian Reynaldo Angulo y Edgar Alonso Bojaca Garavito, gracias por su orientación, estoicismo y disponibilidad para orientarme.
Finalmente, a la Universidad Nacional a Distancia UNAD, Facultad de Ingeniería y Ciencias Básicas, porque me ha permitido ser, expresarme y continuar haciendo lo que me apasiona.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

INTRODUCCION

Hablar hoy de ingeniería social es más frecuente de lo que parece, pues surge como todo un proceso dedicado a intervenir en las actitudes, relaciones y acciones de la humanidad. Esta afecta a todos en la sociedad, pero se enfoca principalmente a las empresas u organizaciones que manejan gran tipo de información; las organizaciones más sensibles a un ataque de ingeniería social son las del sector bancario, puesto que manejan recursos económicos. Siendo el método más utilizado: El Phishing.

El presente trabajo tiene como objetivo conocer en qué consiste la ingeniería social, cómo afecta a las grandes empresas colombianas sobre todo a las distribuidoras de productos de alto consumo y cuáles son las medidas que estas toman para mitigar los riesgos ante la misma.

Para llevar a cabo el presente trabajo se ha partido de la importancia que ha tomado la tecnología y la informática en todos los procesos de la sociedad y la influencia que esta puede llegar a tener en la vida de las personas. Se citan casos presentados en algunas empresas colombianas, se desglosan los tipos de ingeniería utilizados desde las personas y desde la web, las metodologías y se hacen algunas recomendaciones para afrontar los conflictos que se presentan en relación con el cibercrimen.

Igualmente, se busca dejar claro que, para llevar a cabo un ataque de ingeniería social, no es necesario tener conocimientos técnicos o formación en el campo, basta con contar con buenas habilidades sociales y malas intenciones para acceder a la información sensible, pero crucial de cualquier organización.

La investigación se desarrolla desde las siguientes categorías: ingeniería social, comunicación, sistema, seguridad y confianza. En la referencia teórica se hace lectura de autores como Ana Arbeláez, Edgar Castellanos y Jair Sandoval, Cristian Borghello, David Franco, Walter hidalgo, César Jaramillo, David López y José Manuel Orrego.

1. RESUMEN

Hoy hablar de ciber seguridad es vital, la sociedad se encuentra en un momento donde la tecnología es el auge del desarrollo y el internet transversaliza el mismo.

Por naturaleza el ser humano tiende a proteger lo que considera suyo y confía en que personas, espacios o lugares en donde entrega su información le brinde seguridad y confianza ante la misma.

Las empresas colombianas poseen gran información de la población y están constantemente vulnerables a ataques. Las mismas, asiduamente plantean nuevas estrategias: antivirus, sistemas de bloqueos, detención, etc… sin embargo, no desconocen que hay otro tipo de manipulación de la tendencia humana para usar la información sensible y es la Ingeniería Social, ésta en lugar de lidiar con las complejas protecciones instaladas, engañan a los miembros de la organización. Por eso se hace urgente una debida información y formación al respecto.

El presente trabajo busca presentar las Técnicas de Ingeniería Social a las que son vulnerables las Grandes Empresas Colombianas y como se pueden prevenir, muchas de los cuales, han existido hace tiempo y otras que han surgido y tienen gran éxito.

2. PLANTEAMIENTO DEL PROBLEMA

2.1 DESCRIPCION

Se hace importante interpretar o visualizar de otra manera la realidad circundante de las organizaciones y/o empresas colombianas. Hoy es inevitable hablar de la importancia que ha tomado la tecnología y la informática en todos los procesos para las diversas organizaciones. El mundo organizacional tiene una gran obligación entre y para la sociedad, éste cada día almacena grandes cantidades de información y la misma es importante en diversos grados; sin embargo y ante el vertiginoso cambio, se hace urgente posibilitar la protección de la misma sin importar como se recolecte: física o digital; llámese ésta protección en el ámbito empresarial, hacer uso de salvaguardas. Cabe recordar que la información es el eje central de la organización y esta recolecta, datos financieros, personales, comerciales, técnicos, entre otros. Teniendo en cuenta lo anterior se hace necesario conocer los riesgos y plantear nuevas estrategias de seguridad en las organizaciones, puesto que son muy vulnerables a la perdida, robo o secuestro de la Información.

Es necesario tener en cuenta que a medida que se posibilitan herramientas y aplicaciones que hacen más ágil el trabajo y lo facilitan más organizado, también surgen otras que amenazan la seguridad y buscan ser obstáculo en el proceso; es aquí, donde aparecen personas mal intencionadas con programas que ciberatacan la información, éstas conocidas como Hackers, Copyhackers y los Phreak, todos caracterizados por poseer altos conocimientos en el área de la tecnología.

Por otro lado, si una empresa quiere ser competitiva en la actualidad debe contar con sistemas y plataformas súper ágiles y seguras y esto conlleva un cambio en el proceso de transformación digital. Pero de nada sirve tener los mejores sistemas de protección, sino se cuenta con personal idóneo y seguro de su labor, personas con astucia y formación para sospechar ante la presencia de terceros sin escrúpulos que solo buscan perjudicar la organización como tal. Los ciber delincuentes están listos a aprovechar cualquier oportunidad que se les presente para agredir y cada día la *Ingeniería Social* es más utilizada para este tipo de ataques. Por tanto, es necesario que las empresas le den la importancia que se merece la *Protección de la Información* y sensibilice a todo su personal de la gran responsabilidad que se tiene y tome conciencia de que la seguridad se fundamente en la confianza. .

2.2 FORMULACION

Dado todo lo anterior, este trabajo busca responder la siguiente cuestión ¿Qué estrategias se deben implementar en las empresas colombianas distribuidoras de productos de alto consumo y rotación; para prevenir y/o disminuir el riesgo de ataques de ingeniería social?

3. JUSTIFICACION

Día a día las Grandes Empresas Colombianas son más vulnerables al robo, pérdida o secuestro del activo más importante y valioso que tienen: *la información* y por lo general no basta con los controles físicos y lógicos que se tienen para la protección de éste. Por medio de una llamada, un correo, páginas web falsas, entre otros. Los ciber delincuentes están atentos a utilizar la *Ingeniería Social* para persuadir la buena voluntad de las personas o empleados y de esta manera obtener información vital y confidencial como: contraseñas, cuentas bancarias. En algunas ocasiones esta información es utilizada posteriormente para realizar otro tipo de ataques más sofisticados y en otras ocasiones hasta se vende al mejor postor, en este caso la competencia en el mercado.

Entre estos ataques o mal uso de la ingeniería se destaca el *phishing*, el cual se basa en incitar al usuario para que ingrese a una página falsa, habitualmente asociada con una entidad financiera y obtener información privilegiada.

Por todo esto, es muy importante que las Grandes Empresas Colombianas además de tener buenos controles físicos y lógicos, se estén actualizando cada día de las Técnicas de Ingeniería Social y de cómo prevenirlas; así mismo, se requiere capacitación constante y socialización de las nuevas formas de ataques.

Hoy se busca productividad, eficacia y eficiencia por parte de las organizaciones, conllevando a que sea primordial la custodia de la información y de esta manera satisfacer a los demandantes de la oferta. Pero esto no se puede lograr sino se conoce de antemano los riesgos y las vulnerabilidades que también se actualizan.

Este trabajo tiene como fin presentar las técnicas de ingeniería social que se aplican a las grandes empresas colombianas y como se pueden prevenir. A partir de una información recolectada, póstumo análisis y pautas de prevención.

4. DELIMITACION Y ALCANCE DEL PROYECTO

El sector para trabajar es el de las grandes empresas colombianas distribuidoras de productos de alto consumo y rotación, ubicadas en la ciudad de Medellín, puesto que a mayor infraestructura, personal, responsabilidad, información, activos, bases de datos, etc, mayor es el riesgo que se corre de sufrir un ataque informático.

Por otra parte, se identifican los ataques más utilizados en ingeniería social, y las pautas para reducir los riesgos, teniendo en cuenta algunas prácticas de seguridad informática, recomendadas por expertos en el tema.

El fin del proyecto es conocer y tomar cada vez mayores controles respecto a la información que se maneja en la red y/o digital; de tal manera, que se minorice la facilidad con la que los ciberdelincuentes alcanzan sus objetivos, que no siempre significan un beneficio económico.

5. OBJETIVOS

5.1 OBJETIVO GENERAL

Evaluar las vulnerabilidades en seguridad informática desde la ingeniería social en las grandes empresas colombianas distribuidoras de productos de alto consumo y rotación, estableciendo algunas pautas para prevenir los ataques.

5.2 OBJETIVOS ESPECIFICOS

- Determinar los tipos y técnicas de ingeniería social y sus riesgos.

- Categorizar las vulnerabilidades en seguridad informática de las grandes empresas.

- Establecer las formas de prevención hacia este tipo de ataques.

6. MARCO REFERENCIAL

6.1 MARCO TEORICO

Para efectos comprensivos, es importante iniciar proponiendo las categorías sobre las cuales se realiza el presente trabajo: ingeniería social, comunicación, sistema, seguridad y confianza; para comprenderlos se propone hacer lectura de autores como Ana Arbeláez, Edgar Castellanos y Jair Sandoval, Cristian Borghello, David Franco, Walter hidalgo, César Jaramillo, David López y José Manuel Orrego.

Aunque hay que admitir que en cuestión de tecnología y desarrollo se utilizan infinidad de herramientas, unas más válidas que otras, pero todas manipuladas por seres humanos. Si retomamos los orígenes de la computación no encontramos que los fines de creación no fueron tan perfectos, como la utilidad que nos favorece en el momento y sus fines eran realmente funestos. Pero a la vez que esto se ha ido depurando y fortaleciendo, han surgido otra serie de estrategias o instrumentos que "*desafían al sistema falsamente infalible*" [1] y lo más irónico es que utiliza al mismo sujeto para su beneficio y como se cuestiona el mismo autor, ¿hablamos de ingeniería social o simple fraude?

"Se trata de que usted está dando su consentimiento para ser atacado, para ser engañado con su beneplácito y, lo más irónico, es que usted es quien sienta a la mesa a su verdugo. ¡Qué bajo ha caído el enemigo! Se ha perdido todo el honor – ¿A quién puedo reclamar, si he sido yo el anfitrión? Los nuevos hackers cada vez saben menos de informática y más de psicología, porque hoy en día resulta más fácil engañar a una persona que a todo un sistema blindado con antivirus, cortafuegos y otras sutiles herramientas defensivas. Los refinados estafadores juegan con nuestras debilidades, y la principal de ellas es la impaciencia"[2].

Por todo lo mencionado y las constantes amenazas que se presentan ocasionando la fuga y perdida de información, algunas organizaciones internacionales presentaron algunas medidas para la seguridad de la información, entre ellas Normas ISO 27001:2013 Y 27002:2015 Sistemas de Gestión y

[1] ORREGO, Jose Manuel. Ingeniería Social o simple estafa [en línea]. Revistavenamerica.com. (8 de mayo de 2017). [Consultado: 1 de junio de 2018]. Disponible en Internet: https://revistavenamerica.com/ingenieria-social-o-simple-estafa/

[2] ORREGO, Jose Manuel. Ingeniería Social o simple estafa [en línea]. Revistavenamerica.com. (8 de mayo de 2017). [Consultado: 1 de junio de 2018]. Disponible en Internet: https://revistavenamerica.com/ingenieria-social-o-simple-estafa/

Seguridad de la Información. La primera es una norma global, integral y se relaciona bien con otras normas. No cómo sebe implementar, sino que debe hacer cada organización, dependiendo de sus prioridades. Por eso es flexible. La segunda establece las directrices y principios generales para la implementación, el mantenimiento y la mejora del sistema. Con todo esto se busca productividad, eficacia y eficiencia por parte de las organizaciones, conllevando a que sea primordial la custodia de la información y de esta manera satisfacer a los demandantes de la oferta.

Igualmente, cabe tener presente que el impacto del Cibercrimen es global, afecta a todo mundo, no únicamente a las organizaciones legalmente constituidas. Una organización con un buen SGSI (Sistema de Gestión de Seguridad en la Información) puede prevenir los ataques informáticos, más no se puede decir que nunca vaya a sufrir uno, pero si se hará menos vulnerable ante una amenaza. Así mismo, es importante recordar que el proceso de trasformación frente a seguridad informática debe ser constante, puesto que los pilares de la seguridad en la información son la confidencialidad, integridad y disponibilidad. El mundo informático avanza vertiginosamente y a la par sus atacantes. Los ataques de ingeniería social buscan las grandes empresas como objetivo, puesto que estas pueden tener mayores inconvenientes a la hora de guardar información, por todo aquello de infraestructuras de red y cantidades de usuarios. A mayor complejidad de los sistemas de seguridad, mayor tiempo de investigación del salteador, pero si utiliza la ingeniería social como herramienta se remitirá hacer la misma investigación, pero con los empleados y obtendrá resultados más rápidos.

6.2 MARCO CONCEPTUAL

6.2.1 Ingeniería Social. No se puede hablar de seguridad e información de una forma aislada de la vida del ser humano, él es quien, maneja y direcciona la misma. Igualmente, no podemos desligar estos conceptos de la formación o educación, puesto que se da en los diversos escenarios en los que el sujeto interacciona y se forma.

Sin embargo, este trabajo tiene su atención en algunas empresas colombianas, espacios que almacenan cantidad y vital información de la población y la cual requiere ser salvaguardada de todas las maneras posibles.

Las organizaciones están compuestas de eslabones humanos, susceptibles y vulnerables desde la confianza y justo de este aspecto es que abusan aquellos

que hacen uso de la ingeniería social, aquí se hace necesario tener en cuenta lo que dice Ana Arbeláez, en su texto:

"La ingeniería social es una técnica de hackeo utilizada para sustraer información a otras personas teniendo como base la interacción social, de tal manera que la persona vulnerada no se dé cuenta cómo y cuándo dio todos los datos necesarios para terminar siendo la víctima de un ataque informático. En esta práctica se recurre, principalmente, a la manipulación de la psicología humana mediante el engaño. El delincuente actúa a partir de la premisa de que, en la cadena de seguridad de la información, el ser humano es el eslabón más débil"[3].

Por otro lado, Cristian Borguello, comenta que se trata de engañar y lograr la confianza de la persona que tiene relación con algún sistema[4]. *Y José Manuel Orrego menciona* "El término acuñado por la informática, aunque suene elevado o pretencioso, no es otra cosa que técnicas psicológicas para engañarle. Manténgase alerta y rechace inocentes regalos"[5].

"Por su parte, para Microsoft *El objetivo de un hacker que emplea ingeniería social, alguien que trata de obtener acceso no autorizado a sistemas de cómputo, es similar al de cualquier otro tipo de hacker: quiere el dinero, la información o los recursos de TI de una organización"*[6].

Así mismo es interesante compartir las palabras del Dr. Brad Sagarin, psicólogo social quien manifiesta:
"No hay nada mágico en la ingeniería social. El ingeniero social emplea las mismas técnicas de persuasión que utilizamos todos los demás a diario. Adquirimos normas. Intentamos ganar credibilidad. Exigimos obligaciones

---

[3] ARBELÁEZ, Ana. Ingeniería Social: El Hackeo Silencioso [en línea]. Enter.co. (s.f.). [Consultado: 1 de junio de 2018]. Disponible en Internet: http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/

[4] BORGHELLO, Cristian. El arma infalible: la Ingeniería Social [en línea]. Eset-la.com. (13 de abril de 2009). [Consultado: 30 de mayo de 2018]. Disponible en Internet: http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

[5] ORREGO, Jose Manuel. Ingeniería Social o simple estafa [en línea]. Revistavenamerica.com. (8 de mayo de 2017). [Consultado: 1 de junio de 2018]. Disponible en Internet: https://revistavenamerica.com/ingenieria-social-o-simple-estafa/

[6] JAMES SCOTT, Spencer. Ingeniería Social: eludiendo el "firewall humano" [en línea]. (21 de enero de 2011). [Consultado: 3 de junio de 2018]. Disponible en Internet: http://www.magazcitum.com.mx/?p=1173#.W9e4w3tKjIU

recíprocas. Pero el ingeniero social aplica estas técnicas de una manera manipuladora, engañosa y muy poco ética, a menudo con efectos devastadores"[7].

Continuando, el mismo autor plantea algunas maneras en que basa el ingeniero social su plan y estos pueden ser de actitud, de comportamiento, de apariencia, de habla, etc… y a esto le llama los rasgos de un rol. Lo anterior se debe, a que el ser humano es dado a dejarse llevar en muchas ocasiones por las apariencias y atribuye roles por lo que simplemente ve. No considera la prudencia ante la información como parte fundamental. El primer paso del atacante es crear credibilidad, debe estar seguro del rol que está presentando y simula una cantidad de situaciones que envuelven, distrae y convence. El atacante logra manipular, provocar casi que la sumisión, para obtener la información. Obviamente, nadie espera ser manipulado y engañado, es por eso que tomar a alguien desprevenido es la mejor opción.

"La ingeniería social es utilizada principalmente por genios informáticos, hackers o personas del común, que buscan ser reconocidos, también, las técnicas de ingeniería social son utilizadas por mafias organizadas de cibercriminales que aprovechan para utilizar la información conseguida para aumentar sus actividades ilícitas y sus recursos económicos.

Quizás es el ámbito económico el que más estimula a los atacantes a cometer algún delito. Poder clonar tarjetas de crédito o débito, intervenir sitios de comercio electrónico o bancos para desviar las transacciones, o secuestrar la información de compañías o particulares para exigir un pago a cambio de su devolución, o de lo contrario, amenazan con destruirla; son algunos de los hechos más frecuentes en lo referente al dinero.

Otros atacantes están convencidos, y persuaden a los demás, de sus doctrinas políticas o religiosas, por las que son capaces de vulnerar sitios gubernamentales o privados. Este caso se vio recientemente en Colombia cuando se descubrió por parte de la Policía Nacional una empresa fachada donde el "hacker" Andrés Sepúlveda dirigía una seria de interceptaciones a celulares y otros dispositivos pertenecientes a figuras políticas del ámbito nacional.

[7] MITNICK, Kevin D. y SIMÓN, William L. El arte de la instrucción, cómo ser un hackers o evitarlos [en línea]. Es.slideshare.net. México. (2007). [Consultado: 4 de junio de 2018]. Disponible en Internet: https://es.slideshare.net/kissees/elartedelaintrusion-kevinmitnick

Hay quienes ejecutan sus ataques por puro compromiso, inclusive por diversión, y el resto, por la satisfacción personal de ser reconocidos públicamente o por su propia comunidad, tratando de imponer hitos cada vez más altos que representen un reto para los futuros delincuentes informáticos.

Existen diferentes roles en la delincuencia informática, aunque comúnmente, los usuarios corrientes solo reconozcan a los "*hackers*" como los únicos atacantes de sus computadoras. Cada uno cuenta con sus propios distintivos y juegan un papel determinado en cada forma de vulnerar la seguridad de la información"[8].

En el 2009 mediante la ley 1273 Colombia realizó un trabajo de estandarización de los delitos informáticos, mencionado "de la protección de la información y de los datos". la misma, está dividida en dos capítulos: *De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos* y *de los atentados informáticos y otras infracciones*. A continuación, se presentan los 9 delitos tipificados en la ley:

- "Acceso abusivo a un sistema informático.
- Obstaculización ilegítima de sistema informático o red de telecomunicación.
- Interceptación de datos informáticos.
- Daño Informático.
- Uso de software malicioso.
- Violación de datos personales.
- Suplantación de sitios web para capturar datos personales.
- Hurto por medios informáticos y semejantes.
- Transferencia no consentida de activos"[9].

6.2.2 Categorías de ataques en la ingeniería social. Cuando hablamos de ingeniería social inmediatamente pensamos en robo de información, pero también debemos tener en cuenta que existen diferentes categorías en las cuales podemos posicionar los diferentes ciberataques como son estos dos grupos:

- **"Hunting:** Son aquellos ataques que buscan obtener información específica del objetivo con la menor exposición directa posible**.** Con el menor contacto. En la práctica hablamos de ataques de ingeniería social enfocados a obtener

[8] PLAZAS GARCIA, Edna Rocio. Trabajo de grado: Ingeniería Social en las Empresas Colombianas [en línea]. Stadium.unad.edu.co. (2018). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

[9] REY, Jhonny. Deontología Informática [en línea]. Delitosinformatico2580.blogspot.com. (2 de noviembre de 2010). [Consultado: 30 de mayo de 2018]. Disponible en Internet: http://delitosinformatico2580.blogspot.com/

X dato (normalmente credenciales de acceso a un servicio o cuenta, activación o desactivación de alguna configuración que puede complicar el objetivo final o como apoyo a un ataque mayor, dirigido y persistente), de forma que el atacante se pone en contacto de alguna manera con la víctima, y la insta a realizar una acción cuyo desenlace es el pretendido inicialmente.

- **Farming:** Pues justo lo contrario. En el **hunting** lo que se busca es una exposición mínima. Obtener algo y desaparecer. Con el **farming** el objetivo es mantener el engaño el mayor tiempo posible, para exprimir al máximo el conocimiento, recursos o posición de la víctima. Para ello, se suele recurrir a granjas de identidades, que por lo general han sido robadas con anterioridad"[10].

6.2.3 Aspectos claves en la ingeniería social. En primer lugar, tenemos la que se basa en la tecnología, el hacker engaña al usuario utilizando la interacción por medio de una aplicación o sistema que él mismo controla. Entre esto se tiene:

Según Kevin Mitnick, "el éxito de los ataques de ingeniería social se debe a cuatro principios básicos y comunes a todas las personas:

- Todos queremos ayudar.
- El primer movimiento es siempre de confianza hacia el otro.
- No nos gusta decir **No**.
- A todos nos gusta que nos alaben"[11].

De acuerdo con lo anterior la ingeniería social tiene dos puntos clave en los que se basa el ciberdelincuente para realizar el ataque, ellos son la psicología (ya que por medio de halagos etc., pueden acceder a nosotros) y la interacción social ya que mediante las redes o la interacción con intrusos se logra el objetivo.

6.2.4 Tipos y técnicas de ingeniería social. En primer lugar, tenemos la que se basa en la tecnología, el hacker engaña al usuario utilizando la interacción por medio de una aplicación o sistema que él mismo controla. Entre esto se tiene:

---

[10] IGLESIAS, Pablo F. #Mundo Hacker: Los 6 principios básicos de la ingeniería social [en línea]. Pabloyglesias.com. (s.f.). [Consultado: 18 de noviembre de 2018]. Disponible en Internet: https://www.pabloyglesias.com/mundohacker-ingenieria-social/

[11] PISCITELLI, Emiliano. Ingeniería Social: Cuáles son los tipos de ataque [en línea]. Redusers.com. (4 de diciembre de 2015). [Consultado: 18 de noviembre de 2018]. Disponible en Internet: http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/

- **El correo spam:** Mensaje que ofrecen diversos productos y tiene como objetivo instalar un código malicioso al momento en que el usuario abra el archivo.

- **Ventanas emergentes:** Ventanas falsas creadas para distraer al usuario.

- **Software:** Convencer al usuario para la instalación de programas aparentemente legítimos.

- **Phishing**: En incitar al usuario para que ingrese a una página falsa, habitualmente asociada con una entidad financiera y obtener información privilegiada. En segundo lugar, se presenta la del engaño humano, más difíciles de detectar, pero más eficaces, justo esta aprovecha la fragilidad de los sujetos, entre algunas se tiene:

- **Dumpster Diving:** Análisis por parte del hacker de la "basura" organizacional, de donde puede obtener listas, teléfonos, reportes, etc…de ahí que hasta la información que no se considere necesaria y/o importante debe ser desechada de manera segura.

- **Pre-texting:** Creación de un escenario falso para la persuasión del ser humano, logrando la confianza y credibilidad necesaria para alcanzar su propósito.

- **"Shoulder surfing**: Es una técnica muy empleada y consiste en espiar "sobre el hombro" (de ahí su nombre) a los usuarios cuando teclean su nombre y contraseña en algún sistema"[12].

- **Ingeniería social inversa:** Estrategia más avanzada, se trata de la creación de un personaje con mayor autoridad por parte del hacker, lo cual permite obtener información poderosa. Esta "tiene tres grandes etapas:

[12] JAMES SCOTT, Spencer. Ingeniería Social: eludiendo el "firewall humano" [en línea]. (21 de enero de 2011). [Consultado: 3 de junio de 2018]. Disponible en Internet: http://www.magazcitum.com.mx/?p=1173#.W9e4w3tKjIU

sabotaje, anuncio y asistencia"[13]. Requiere de mayor preparación y tiempo pata ejecutarla.

6.2.5 Metodología de la ingeniería social. La metodología aplicada en la Ingeniería Social consta de las siguientes fases:

- **"Fase de acercamiento:** Se hace el primer acercamiento al objetivo para ganar su confianza. Generalmente, el atacante que se vale de la ingeniería social permite al objetivo dominar la comunicación porque así detecta sus debilidades primarias a ser explotadas.

- **Fase de alerta:** Seguido, plantea varias opciones al objetivo para medir y observar su velocidad de respuesta bajo presión. En esta etapa, su grado de interacción cambia y comienza a ser más activo: Lanza proposiciones sueltas aquí y allá; todas especialmente pensadas para afianzar la confianza inicialmente establecida. Con ellas logrará que el objetivo revele más información de la que generalmente está dispuesta a entregar.

- **Fase de distracción:** En esta fase; el atacante ya ha consolidado gran parte de la confianza que necesita para conseguir que el objetivo revele los datos que le interesan. El objetivo se siente a gusto en la comunicación y baja sus defensas a niveles penetrables. En paralelo, el atacante domina prácticamente la comunicación; si bien no llega al punto de agobiar al objetivo para evitar que éste levante sus alarmas.

  Con esto en mente, se dedica a tranquilizar al objetivo con promesas o frases de confianza que terminan de derribar sus barreras. Como parte natural de la interacción y ya completamente envuelto por el atacante; el objetivo termina entregando datos sensibles como por ejemplo, claves de acceso a cuentas o números de seguridad de sus tarjetas de crédito.

  Esta metodología ha probado ser extremadamente poderosa porque mina la defensa de los objetivos quienes, además de perder dinero y su privacidad; también pierden la confianza en sí mismo y en sus capacidades"[14].

[13] JAMES SCOTT, Spencer. Ingeniería Social: eludiendo el "firewall humano" [en línea]. (21 de enero de 2011). [Consultado: 3 de junio de 2018]. Disponible en Internet: http://www.magazcitum.com.mx/?p=1173#.W9e4w3tKjIU

Estas fases las podemos entender más claramente con el siguiente paso a paso que utiliza el atacante:

- **Identificar a la víctima:** Esta es la actividad inicial antes de ejecutar el ataque de ingeniería social. El hacker plantea el objetivo y estima las probabilidades de éxito que puede tener ese ataque, este ataque se puede dar a una empresa, organización o persona.

- **Reconocimiento:** El hacker comienza la búsqueda de datos sobre la víctima, que le puedan servir para su ataque.

- **Crear el escenario:** Se realiza la configuración del escenario del ataque, depende del ingenio del hacker y sus habilidades para burlar la seguridad con que cuenta la víctima, las instalaciones físicas y sistemáticas que existen en las empresas, las cuales ya ha estudiado en el paso anterior y sabe cuáles son sus puntos más vulnerables

- **Realizar el ataque**: El hacker pone en práctica técnicas como lo que es la ingeniería social inversa, como también el uso de diferente software, como lo son los keyloggers y los sniffers, realiza el escaneo de puertos y el de identificar y analizar los mapeos de redes, el phishing y también el de ganarse la confianza de la víctima para cumplir con sus objetivos establecidos.

- **Obtener la información:** Es donde se realiza el control de la situación, como también de la red y del ordenador, el hacker con sus habilidades de ingeniería social procede a captar la información que necesita, ya sea por medio de un ordenador, de una memoria USB, de un teléfono inteligente, una cámara digital o también con herramientas informáticas, como lo es un malware, el cual permite enviar constantemente los datos a una dirección de correo electrónico o a una dirección IP.

- **Salir del proceso de ataque:** una vez cumplido con los objetivos establecidos del ataque por parte del hacker (que en la mayoría son los hackers de sombrero negro y grises o crackers) este abandona el lugar o la situación sin levantar sospecha, pero desde luego se debe quemar toda la evidencia, como,

---

[14] MENDOZA, Azury. Conoce los riesgos y amenazas de la Ingeniería social sobre los activos y datos sensibles [en línea]. Gb-advisors.com. (27 de febrero de 2018). [Consultado: 28 de octubre de 2018]. Disponible en Internet: http://www.gb-advisors.com/es/riesgos-y-amenazas-de-la-ingenieria-social/

por ejemplo, las memorias RAM, disco duro, la placa madre o Board, entre otros elementos de hardware, el cual puede dejar evidencia del ataque.

6.2.6 Objetivos de la ingeniería social. Los ciber-delincuentes actúan de manera premeditada y atacan directamente los sistemas internos de las organizaciones, su objetivo es afectar la imagen de las compañías a través de los fraudes; se valen de los puntos vulnerables en la seguridad tecnológica de la empresa, logrando así, conocer los datos que necesita.

Igualmente, los ciber-delincuentes a través de las técnicas conocidas buscan lucrarse económicamente. Solo necesita un mediano o alto conocimiento de computadores y redes y saber diferenciar entre la información que necesita y el método a utilizar. Son personas con una alta capacidad de interactuar y desde la confianza ganada sondear los datos de clientes e información confidencial.

Algunos de los desafueros que se presentan en este tipo de situaciones son:

- Hackeo de Redes Sociales como Facebook, Instagram, WhatsApp, etc.
- Suplantación de identidad para compras en Internet.
- Obtención de cuentas de correos para enviar correos Spam y realizar trámites ilegales.
- Daño de ordenadores y datos, afectando los servicios de las empresas.

6.2.7 Los más vulnerables a la ingeniería social. En un mundo tan globalizado nadie está exento a sufrir algún incidente de ciberseguridad. El cibercrimen, es hoy una de las principales amenazas a la economía mundial y las PYMES son cada vez más afectadas. Son muchos los aspectos que posibilitan un ataque desde la Ingeniería Social y para la misma no hay victima pequeña, puesto que lo que se mueve detrás, son colectivos y mafias que desean sacar beneficio sin importar a quien se dañe.

Como se menciona anteriormente en el trabajo la ingeniería social ha cobrado gran importancia gracias a la expansión del uso del internet en las diversas realidades en que nos encontramos inmersos, negocios, entretenimiento, salud, industria, deporte, etc. Se aprovecha de la confianza para acceder sin previo

consentimiento a la información que necesita. La agilidad de los ciber-delincuentes, aprovechan hasta la mínima oportunidad para alcanzar su objetivo.

Algunas de las situaciones que se presentan en la cotidianidad y que son aprovechadas por el cibercrimen, son:

- Empleados que inconscientemente proporcionan información confidencial por medio de un correo electrónico y/o llamadas telefónicas.
- Personas que realizan transacciones relacionadas con la banca.
- Publicación de artículos, películas y/o música.
- Descarga de imágenes o archivos de remitentes desconocidos.
- La poca inversión de las empresas a la Seguridad de la Información.
- Publicación de datos personales en redes sociales.
- Utilización de contraseñas no seguras.

Siendo así nadie está a salvo de un ataque de Ingeniería Social; por tanto, la prevención debe ser la primera medida de seguridad y de esta manera hacer frente a las amenazas cibernéticas. Cabe anotar que las grandes empresas son más vulnerables a este tipo de ataques debido a la cantidad de información, infraestructura TI y personal que manejan.

7. ATAQUES DE INGENIERIA SOCIAL A LAS GRANDES EMPRESAS COLOMBIANAS

El cibercrimen es una amenaza cada vez más latente en Colombia, afectando la seguridad, la economía, la tranquilidad de las personas que, a pesar de la mucha información para hacer frente al mismo, no tienen formación y se continúa cayendo en este tipo de trampa. Como se menciona en la revista semana "los delitos en la red aumentaron un 28% durante 2017 y causaron pérdidas superiores a los 50 mil millones de pesos"[15].

"Según los informes entregados por el Centro Cibernético de la Policía Nacional, durante los últimos 3 años se presentaron 15.565 denuncias por incidentes informáticos en Colombia. Las víctimas de estos ataques de ingeniería social cambiaron en los últimos años, pasando de afectar al ciudadano de a pie, a afectar a las grandes empresas del sector público y el sector privado, las cuales generan una mayor rentabilidad a la actividad criminal"[16].

Tabla 1. Porcentaje de denuncias por incidentes informáticos en Colombia entre el año 2014 y 2017

Sector	2014	2015	2016	2014-2017
Ciudadano	92%	63%	57%	66%
Financiero	5%	15%	14%	12%
Industrial		5%	7%	5%
Tecnología		4%	8%	6%
Gobierno		6%	2%	3%
Educación		3%	4%	3%
Medios de Comunicación		2%	4%	3%
Menor de Edad		2%	3%	2%
Salud		0%	1%	

Fuente. El Autor

"En el 2014, del total de incidentes atendidos, el 92% afectaban a los ciudadanos del común, para el 2015 el 63% y en el 2016 el 57%, presentando una disminución

[15] SEMANA. El Cibercrimen en 2017: La amenaza crece sobre Colombia [en línea]. Semana.com. (28 de diciembre de 2017). [Consultado: 28 de octubre de 2018]. Disponible en Internet: https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979

[16] POLICIA NACIONAL. Informe: Amenazas del Cibercrimen en Colombia 2016-2017 [en línea]. Caivirtual.policia.gov.co. (marzo 2018). [Consultado: 28 de octubre de 2018]. Disponible en Internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

del 35%. Mientras tanto, el sector empresarial pasó de un 5% a un incremento del 28% en los reportes atendidos"[17].

7.1 METODO DE INGENIERIA SOCIAL MAS UTILIZADO EN COLOMBIA

"En un año en Colombia, se registran cerca de 198 millones de ataques cibernéticos, es decir, 542.465 ataques diarios".[18] De esta manera Colombia ocupa el tercer puesto entre los países afectados por este tipo de delitos en toda Latinoamérica.

Tabla 2. Porcentaje de ataques informáticos que ocurren diariamente en Colombia

Sector	%
Financiero	40
Telecomunicaciones	26
Gobierno	15
Energético	4
Industria	9
Retail	6

Fuente. El Autor

"Según un estudio realizado por Karpersky lab, los usuarios de los países de Brasil, México y Colombia han registrado el mayor número de ataques informáticos en lo que va del 2017"[19].

"Una de las técnicas más utilizadas para robar los datos de una compañía es la ingeniería social. Según Patricia Gaviria, directora de educación de ETEK

[17] POLICIA NACIONAL. Informe: Amenazas del Cibercrimen en Colombia 2016-2017 [en línea]. Caivirtual.policia.gov.co. (marzo 2018). [Consultado: 28 de octubre de 2018]. Disponible en Internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

[18] DINERO. Los sectores económicos más impactados por el cibercrimen en Colombia [en línea]. Dinero.com. (26 de septiembre de 2017). [Consultado: 2 de noviembre de 2018]. Disponible en Internet: http://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321.

[19] KASPERSKY LAB. 33 ataques por segundo: Kaspersky Lab registra un aumento del 59% en ataques de malware en América Latina [en línea]. Latam.kaspersky.com. (s.f.). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://latam.kaspersky.com/about/press-releases/2017_33-attacks-per-second-increase-in-malware-attacks-in-latin-america

International, esta es una técnica utilizada por varios delincuentes para extraer información confidencial o información sensible de las empresas.

El método de ingeniería social más utilizado por los ciber delincuentes es el 'phishing', que consiste en suplantar cualquier tipo de página web para robar información crediticia o personal.

¿Qué información roba phishing? y ¿Cómo se distribuye?

Figura 1 Prototipo del phishing

Fuente: RIVERO, Marcelo. Infospyware.com [imagen]. ¿Qué información roba phishing? y ¿Cómo se distribuye? (consultado: diciembre 6 de 2018) disponible en https://www.infospyware.com/articulos/que-es-el-phishing/.

Circuito de un ataque de phishing.

Figura 2 Circuito de phishing

Fuente: RIVERO, Marcelo. Infospyware.com [imagen]. Circuito de un ataque de phishing. (Consultado: diciembre 6 de 2018) disponible en https://www.infospyware.com/articulos/que-es-el-phishing/.

Este método utilizado por los ciber delincuentes, tiene el objetivo de engañar y así conseguir información personal muy importante (contraseñas, números de tarjetas de créditos, historiales, etc…) Utilizan correos electrónicos falsos o redirigen a sitios web ilusorios.

¿De dónde procede el phishing?

Los diversos mensajes pueden provenir de cualquier parte u empresa legítima, inclusive de su banco; pero ojo, ahí radica el problema, que parecen tan reales que por eso confunden, pues se trata meramente de imitaciones. El mensaje siempre va a sugerir de manera muy jovial que confirme la información de su cuenta, puesto que la misma presenta algún inconveniente y cuando usted accede, le redirecciona a una página falsa.

¿Cómo evitar el phishing?

- No abra correos electrónicos de desconocidos.

- No proporcione información personal a nadie, no importa que porque medio se la soliciten.

- No revele sus contraseñas o números de cuentas.

- Compruebe las URL, a simple vista son legítimas, pero en realidad están camufladas (mal escritas, se adicionan o sustraen letras, etc…).

- Actualice su navegador y utilice parches de seguridad.

- Proteja su equipo con un antivirus y firewall.

- Sea consciente que ninguna empresa u organización le solicitara los datos confidenciales para ningún tipo de transacción.

- Si tiene alguna duda sobre el correo recibido, llame *directamente* a la empresa y solicite información.

La cifra de casos de ingeniería social a través de 'phishing' aumentó un 22,6% entre 2015 y 2016, registrando más de 200 denuncias mensuales. Por su parte, la compañía informática RSA señala que este tipo de ataques cibernéticos aumentan entre un 30% y un 40% cada año.

La falta de implementación de programas de concientización en seguridad de la información a directivos y empleados de las compañías han convertido al 'phishing' en una de las causales de ciber delincuencia más relevantes en 2017; aumentando los riesgos informáticos"[20].

[20] RCN. Pishing, el método de robo por internet más utilizado en el país [en línea]. Noticias.canalrcn.com. (11 de octubre de 2017). [Consultado: 2 de noviembre de 2018]. Disponible en Internet: https://noticias.canalrcn.com/tecnologia-tecnologia/pishing-el-metodo-robo-internet-mas-utilizado-el-pais

7.2 CASOS DE INGENIERIA SOCIAL REPORTADOS POR EMPRESAS COLOMBIANAS

A continuación, se menciona algunos casos de ingeniería social, ocurridos en empresas colombianas en los últimos años.

Entidad Bancaría MasterCard (22 de marzo de 2016): "La compañía de seguridad informática Eset, emitió un comunicado donde habla de una nueva campaña de 'phishing' (modalidad que implementan los cibercriminales para suplantar personas o empresas de confianza) generada para robar datos bancarios.

Para este ataque de phishing los delincuentes informáticos decidieron enviar correos electrónicos falsos a las cuentas de sus víctimas, estos correos simulan ser de la entidad bancaria MasterCard, ya que la dirección oficial (eresumen@masterconsultas.com.ar) tiene un dominio parecido al que usan estos suplantadores, es por esta razón que la víctima piensa que verdaderamente la entidad les envío el correo e ingresan respondiendo a las preguntas que aquí se le hacen.

El correo empieza con el saludo 'Estimado socio', el contenido del mensaje está diseñado para que el usuario crea que tiene problemas con su tarjeta de crédito, por lo que su servicio será suspendido. Al recibir este mensaje la persona se asusta pues piensa que ya no puede hacer pagos con su tarjeta de crédito, entonces procede a aceptar la invitación que aquí se le hace, donde le piden realizar una reactivación del servicio mediante una URL y al momento de hacer clic, es redireccionado a otro sitio web falso. Al ingresar a este nuevo sitio web falso, se le pide a la víctima completar un formulario con los datos personales y los datos bancarios como número de tarjeta y clave que tenía anteriormente. Cuando la víctima carga todos los datos y da clic sobre el botón de validar, toda la información es enviada al ciber atacante para que sea recopilada por el mismo.

Para dar confianza de que la transacción fue hecha el sitio web avisa a la persona que la operación fue exitosa y para disimular un poco direccionada a la víctima a un portal que contiene los enlaces de la página oficial de MasterCard. Este detalla que los proveedores de servicios nunca envían mensajes personalizados como

por ejemplo 'Estimado cliente'. De hecho, las entidades financieras tampoco solicitan a sus usuarios iniciar sesión desde un vínculo integrado en el mensaje"[21].

La recomendación para este tipo de casos de phishing es que las personas nunca deben de proporcionar información bancaria, ni información privada a nadie por medios telefónicos, ni por correos, ni cuando esté hablando con extraños.

Fiscalía General de la Nación (18 de agosto de 2016): "ESET La compañía de seguridad informática de Eslovaquia, informo en agosto de 2016 acerca de un archivo malicioso que se encontraba circulando a través de correo electrónico, donde se escondía un virus que pretendía infectar los computadores de los usuarios a través de un archivo que contenía una falsa citación de la fiscalía colombiana.

Estos piratas informáticos, utilizaban el correo como medio electrónico de comunicación con las víctimas, en los correos que ellos enviaban utilizaban documentos que parecían ser de uso oficial de la Fiscalía General de la Nación, la gente confiaba en que ese documento era de esta entidad del estado ya que estos inteligentes ladrones enviaban la carta con el logo de esa entidad.

En la supuesta citación hay un mensaje que decía, que por no acudir en los tres llamados que se le hicieron a declarar a la fiscalía, el juzgado le había iniciado un proceso penal en el cual se le judicializaría. Con ese pretexto se le pedía a la víctima que ingresara a través de un enlace que ahí se le suministraba, del cual se descargaría la falsa citación que contenía un virus en su interior.

Cuando los usuarios daban clic en el enlace de descarga, se empezaba a descargar un archivo PDF, este archivo era un archivo infectado con un virus llamado Win32/Remtasu.

Ante este tipo de hechos, es bueno que las personas sospechen de este tipo de correos, que no los abran de una, qué en vez de dar clic de una buena vez en el enlace, llamen o se acerquen a la entidad y pregunten si de verdad ellos enviaron ese correo. Ya que, si las personas implementáramos hábitos de seguridad tan sencillos como el poner el puntero del mouse encima de los enlaces que vienen

[21] EL TIEMPO. Alerta por correos falsos que atacan a usuarios de MasterCard y Visa [en línea]. Eltiempo.com. (29 de marzo de 2016). [Consultado: 5 de noviembre de 2018]. Disponible en Internet: http://www.eltiempo.com/archivo/documento/CMS-16549207

dentro de estos correos electrónicos, se podría ver a dónde redirigen realmente el enlacé y se evitaría la perdida de información confidencial"[22].

Bancolombia (13 de marzo de 2017): "La compañía bancaria Bancolombia sufrió un ataque de phishing el pasado mes de marzo, según investigadores de la firma ESET dicen que este ataque aún se encuentra activo y es una gran amenaza para los más de 10.000.000 de usuarios que cuenta la entidad.

Los investigadores informáticos de esa firma advirtieron que los delincuentes informáticos, utilizan un correo falso, llamado informacion@bancolombia.com.co, de donde envían un malware que al ser abierto este le roba los datos de ingreso a la cuenta financiera de los usuarios de Bancolombia, logrando ingresar y desviar el dinero que hay en esas cuentas. La carta enviada por los ciber-delincuentes en la que les manifiestan a los usuarios de este banco, un "supuesto bloqueo de sus productos financieros", invitándolos a restablecer sus cuentas por medio de enlaces que ellos mismos le proporcionan en el mensaje. Si el cliente ingresa por medio de estos links, de una les da el acceso a su cuenta a estos delincuentes.

Los funcionarios del área de sistemas del banco Colombia, sacaron un comunicado en el que le informan a sus clientes que deben de tener mucho cuidado con ese tipo de mensajes que reciben en sus correos, ya que la entidad no acostumbra a enviar ese tipo de mensajes, y los invita a que siempre verifiquen la dirección de la página web a la que van a entrar, para evitar caer en este tipo de engaños.

Las empresas que brindan los servicios de seguridad informática en Colombia invitan a todas las entidades a gastar los recursos económicos necesarios que se necesiten para obtener un buen servicio de ciber-seguridad en sus empresas, ya que estas suelen escatimar en gastos y por eso sufren esos ataques de ingeniería social"[23].

---

[22] PLAZAS GARCIA, Edna Rocio. Trabajo de grado: Ingeniería Social en las Empresas Colombianas [en línea]. Stadium.unad.edu.co. (2018). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

[23] PLAZAS GARCIA, Edna Rocio. Trabajo de grado: Ingeniería Social en las Empresas Colombianas [en línea]. Stadium.unad.edu.co. (2018). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

***Registraduría Nacional del Estado Civil (28 de septiembre de 2016*)**: **"**El registrador nacional Juan Carlos Galindo, dio a conocer a los medios de comunicación que, para septiembre de 2016, la página web de la registraduría nacional del estado civil sufrió cerca de 320 mil ataques informáticos.

Entre ellos uno hecho a los servidores que guardaban la información para las votaciones del plebiscito que se llevarían a cabo el 2 de octubre del mismo año. Según dijo el registrador, con el ataque solo fue afectado el aplicativo que contenía la información al votante, más no el resto de información que guarda la registraduría como documentos de identidad, registros civiles, etc"[24].

Google Docs (5 de mayo de 2017): "Los usuarios que tienen correo electrónico gmail este año sufrieron un ataque de ingeniería social mediante la técnica llamada phishing. Esta técnica consiste en suplantar a un servicio o a una persona.

Para el ataque los victimarios, enviaron un email de alguien que dice haberlos añadido a un documento para trabajar en conjunto, en este mensaje se le pide a la víctima que se haga clic para verlo. Al acceder se le muestra una imagen donde aparecen las diferentes cuentas asociadas a ese trabajo colaborativo.

Cuando el usuario se da cuenta de que es un archivo falso, ya los atacantes han tenido tiempo de hacerse a la información confidencial que ellos necesitan"[25]. "Google reconoció que el ataque ha superado sus medidas de control y protección y recomendó a sus usuarios que solo deben abrir los mensajes para colaborar en un documento de Google Docs si están plenamente seguros de que el remitente es correcto"[26].

---

[24] PLAZAS GARCIA, Edna Rocio. Trabajo de grado: Ingeniería Social en las Empresas Colombianas [en línea]. Stadium.unad.edu.co. (2018). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

[25] PLAZAS GARCIA, Edna Rocio. Trabajo de grado: Ingeniería Social en las Empresas Colombianas [en línea]. Stadium.unad.edu.co. (2018). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

[26] JIMENEZ CANO, Rosa. Google Docs sufre un ataque de 'phishing' [en línea]. Elpais.com. (5 de mayo de 2017). [Consultado: 2 de noviembre de 2018]. Disponible en Internet: https://elpais.com/tecnologia/2017/05/04/actualidad/1493887324_006575.html.

“A los encargados de la seguridad de Google, los tocó tomar medidas de seguridad adecuadas para neutralizar el ataque, entre esas medidas tomadas están:

- Dar de baja las páginas falsas.
- Mantener comunicación con los afectados.
- Trabajar para evitar que vuelva a suceder este tipo de ataques.

La recomendación es que los usuarios deben ir a la página donde se comprueban los permisos de acceso, para revisar qué aplicaciones pueden entrar en nuestro nombre y desactivar todas las que no sean. También se recomienda a los usuarios usar diferentes contraseñas para cada registro”[27].

Dian (17 de octubre de 2017): “El pasado martes 17 de octubre de 2017 la Dirección de Impuestos y Aduanas Nacionales DIAN, emitió un comunicado en donde alertaba a la ciudadanía en general, sobre nuevos ataques de ingeniería social a través de correos falsos que son enviados al correo de las víctimas en nombre de la entidad tributaria, estos correos son enviados por medio de artimañas informáticas, haciendo creer a los ciudadanos que son oficiales, para que los ingenuos ciudadanos caigan en la trampa y den sus datos personales y así poder robarles información confidencial o de cuentas bancarias.

Las cuentas de correo más utilizadas por estos delincuentes son: acastillo@ediagro.com y minhacienda@dian.gov, con asuntos, como: “Hasta la fecha no hemos recibido el pago de sus impuestos”, “Notificación embargo DIAN” y “Problemas con su situación fiscal”, este último mensaje lo recibí el día de hoy 9 de noviembre en mi correo personal.

Sobre el tema de robo por medio de técnicas de ingeniería social, la autoridad tributaria DIAN, recordó a ciudadanos y contribuyentes que, es muy importante validar la información emitida por cualquier entidad ya sea pública o privada y no descargar los archivos adjuntos que envían en estos correos sospechosos para no ser afectado por esta conducta fraudulenta. Así mismo se les recomienda a los usuarios reportar directamente este tipo de malas conductas al Centro Cibernético de la Policía Nacional, para que por medio de las autoridades sean frenados este tipo de ataques de phishing”[28].

---

[27] PLAZAS GARCIA, Edna Rocio. Trabajo de grado: Ingeniería Social en las Empresas Colombianas [en línea]. Stadium.unad.edu.co. (2018). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

[28] PLAZAS GARCIA, Edna Rocio. Trabajo de grado: Ingeniería Social en las Empresas Colombianas [en línea]. Stadium.unad.edu.co. (2018). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

7.3 TIPO DE PAGO A LOS DELINCUENTES INFORMATICOS

"Los hackers que realizan ataques informáticos en todo el mundo ya no piden euros ni dólares para el rescate de esta información, lo que ellos exigen ahora son bitcoins o cualquier clase de criptomonedas.

El bitcoin es una criptomoneda o criptodivisa que se creó en el año 2009. En este momento existen muchos tipos de monedas como estas, entre ellas están: los litecoins, los dogecoins, el bilur, etc"[29].

"Para tener esta moneda virtual, los usuarios deben contar con una aplicación móvil o de escritorio que provee un monedero Bitcoin personal y que permite al usuario enviar y recibir bitcoins"[30].

La autenticidad de cada transacción está protegida por firmas digitales correspondientes a las direcciones de envío, permitiendo a todos los usuarios tener control sobre estos giros.

A modo técnico esto quiere decir que en estas operaciones con estas monedas no hay intermediarios, "se realizan en redes P2P y el cifrado de las transacciones, que son públicas, es tan complejo que resulta muy difícil de rastrear entre quienes se está produciendo el intercambio"[31].

Algunos cibercriminales recurren a servicios de mezclado de bitcoins (mixing) para reducir la probabilidad de ser rastreados. Es como si en un gran grupo de personas que se intercambian monedas participara uno que ha robado una moneda de peso en otro grupo y al mezclar todas las monedas y quedarse el

---

[29] PLAZAS GARCIA, Edna Rocio. Trabajo de grado: Ingeniería Social en las Empresas Colombianas [en línea]. Stadium.unad.edu.co. (2018). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

[30] RPP NOTICIAS. Bitcoin, la moneda virtual que exigen los hackers tras el ciberataque [en línea]. Rpp.pe. (12 de mayo de 2017). [Consultado: 6 de noviembre de 2018]. Disponible en Internet: http://rpp.pe/economia/economia/bitcoin-la-moneda-en-que-piden-rescate-los-hakers-del-ciberataque-mundial-noticia-1050368

[31] HERALDO. ¿Por qué los hackers del ciberataque global exigen los rescates en bitcoins? [en línea]. Heraldo.es. (16 de mayo de 2017). [Consultado: 6 de noviembre de 2018]. Disponible en Internet: http://www.heraldo.es/noticias/sociedad/2017/05/16/por-que-bitcoins-1175631-310.html

ladrón con una ya no se sabe de quién era el peso robado porque todos los pesos son iguales entre sí.

Otra razón por la que el bitcoin llama la atención de los delincuentes informáticos es que “para un cibercriminal el uso de bitcoin resulta muy conveniente porque no tiene que depender del sistema bancario y cuenta con un activo digital muy apreciado con casi $30.000 millones de capitalización”[32].

Una vez recibidos los bitcoins los puede intercambiar en cualquier sitio del mundo por la moneda o activo que más le interese. Por estas razones se recomienda potenciar los usos legales de esta moneda y comprender su funcionamiento para controlar el uso criminal o ilegal.

[32] ESCUDERO RUBIO, Víctor; MARQUEZ SOLIS, Santiago y PREUKSCHAT, Alex. Ciberseguridad cinco claves sobre bitcoin y el ataque informático mundial [en línea]. Retina.elpais.com. (14 de mayo de 2017). [Consultado: 6 de noviembre de 2018]. Disponible en Internet: https://retina.elpais.com/retina/2017/05/12/tendencias/1494619771_719922.html

8. FORMAS DE PREVENCION DE ATAQUES POR INGENIERIA SOCIAL A LAS GRANDES EMPRESAS COLOMBIANAS

“Para disminuir los ataques de ingeniería social en las empresas de Colombia y el mundo entero, se deben tener en cuenta una serie de recomendaciones dadas por los expertos en el tema de seguridad informática, entre esos tips de buenas prácticas están:

- **Agregar a favoritos los sitios web de confianza que se utilizan a diario:** Es recomendable hacerles un tratamiento a las páginas web nuevas a las cuales va ingresar el usuario, como también se le debe hacer seguimiento a las personas que se acaban de conocer en redes sociales y en la calle.
  Del mismo modo en que las personas no confiamos en todas las personas que nos rodean, no se debe confiar inmediatamente de los sitios web que sólo se han visitado una vez. Por medio de esta investigación que se les realiza a las personas y a los sitios web, se puede obtener información confidencial de con quien se va a relacionar o a que sitio se va ingresar y así poder evitar una fuga de información privada.

- **Tener sospechas sobre enlaces que nos compartan a través de redes sociales:** Nunca se debe hacer clic en enlaces sospechosos que nos lleguen a través del correo, Facebook, WhatsApp, o a través de alguna página web a la que se desee ingresar, independientemente de los prometedores mensajes que aparezcan en los avisos de publicidad, no se debe dar clic, porque es como si se estuviera aceptando el robo de la información personal de nosotros mismos. Recuerde que las promesas demasiado buenas están muy lejos de ser verdad.

- **No tener miedo de amenazas:** Las personas no debemos dejarnos intimidar por amenazas recibidas ya sea a través de redes sociales o personalmente. Muchos delincuentes informáticos utilizan ciertos elementos o información confidencial robada, para asustar a sus víctimas y llevarlas a hacer algo en contra de su voluntad, donde las personas terminan haciéndolo solo por temor. Si se siente atemorizado por alguna amenaza, pida ayuda a las autoridades policiales o cuéntele a alguna persona de confianza para que este le ayude.

- **No compartir información con todo el mundo:** No compartamos información confidencial con cualquier persona que se nos cruce en el camino, si se está trabajando en una empresa solo se debe compartir información

confidencial con los jefes, a si se logra que la información esté más protegida y la empresa sea menos vulnerable a ataques de ingeniería social.

- **Prevenir es mejor que curar:** Las empresas colombianas deben de invertir una buena cantidad de dinero en buscar una solución de seguridad informática que proteja su sistema informático y su información confidencial. También se debe explorar y utilizar las opciones de seguridad incorporadas en los sitios web que se visitan a diario, ya que algunos sitios web como Facebook, LinkedIn, twitter, proporcionan información sobre las amenazas a las que estuvieron vulnerables en los últimos días, así mismo da consejos para tener en cuenta a la hora de navegar sobre estas redes sociales y tener nuestros datos protegidos.

- **Denunciar:** Todos los ciudadanos Colombianos tenemos el deber de denunciar cualquier delito, en especial los ataques cibernéticos; esto se hace ante el Centro Cibernético Policial de la DIJIN, dispuesto por la policía nacional para la prevención, orientación y atención de incidentes informáticos que afectan a los Colombianos; este caí virtual funciona las 24 horas de la semana los 365 días del año, a través del portal de servicios: caivirtual.policia.gov.co en el cual se divulgan alertas de ciber-seguridad de las distintas modalidades utilizadas por los delincuentes informáticos en Colombia.

- **Capacitar a los empleados:** Las empresas colombianas ya sean públicas o privadas, deben capacitar al personal de la compañía con programas de Security. Es decir, absolutamente todo el personal que hace parte de la empresa, desde el vigilante, la señora del aseo, las secretarias, los ingenieros del área TIC, hasta los administrativos de alto rango como el gerente, deben estar capacitados en cuanto a los métodos de engaño más practicados por los ciber-atacantes; con el fin de que puedan identificar cuando vayan a hacer víctimas de un ataque de ingeniería social y puedan dar aviso al encargado del área TIC.

- **Backups:** Se deben hacer copias de seguridad de la información que se encuentra en los equipos de una compañía, estos backups se deben hacer periódicamente a través de dispositivos de almacenamiento externos, los cuales deben resguardarse en un lugar diferente al del origen de los datos. Se pueden hacer de forma local o remota a través de infraestructuras y aplicaciones específicas ofrecidas para ello.

- **Imagen del sistema:** Se debe de crear una réplica exacta del disco duro de un equipo ya configurado, a partir de instalaciones limpias, pero también se pueden usar en equipos con datos ya incluidos, a fin de hacer recuperaciones más rápidas en caso de daño de la computadora. Sistemas operativos como Windows 7, 8, 8.1 y 10 incluyen una herramienta para la elaboración de este tipo de respaldos.

- **Cifrado de particiones:** Hacer un cifrado de particiones para hacer ilegible la información contenida en estas, a través de algoritmos matemáticos simétricos, asimétricos o híbridos, esto se debe hacer sobre todo en equipos portátiles.

- **Autenticación:** Se deben crear usuarios y contraseñas seguras, no solo para el acceso al sistema operativo, sino también, a las redes de datos, sistemas de información e inclusive, a la *BIOS* de cada computadora de la empresa. Se debe tener en cuenta la longitud de las contraseñas, caducidad y la complejidad de las contraseñas de acceso atendiendo a las recomendaciones que para ello existen en normas o guías internacionales de seguridad de la información.

- **Actualizar sistemas operativos:** Todos los sistemas operativos de los computadores y de las distintas aplicaciones usadas en la empresa para el desarrollo de las diferentes actividades (contables, financieras, ofimáticas, de comunicación, etc.) deben estar actualizadas o por lo menos contar con los parches ofrecidos directamente por el fabricante. También se debe verificar que en lo posible, esté activada la opción de actualizaciones automáticas en cada software, monitoreando el estado de las respectivas licencias, pues si estas se vencen las actualizaciones no se ejecutarán.

- **Antivirus:** Todos los computadores deben tener un antivirus licenciado y actualizado, ya que estos son una herramienta indispensable a la hora de proteger los datos, a la vez que incluyen una serie de servicios adicionales y complementarios que los convierten en un paquete completo de seguridad.

- **Uso de Firewall:** Los firewalls están en la capacidad de filtrar paquetes a través de reglas establecidas para el tráfico entrante o saliente de los computadores. Lo que se aconseja es hacer una configuración del firewall que

viene por defecto con el sistema operativo y complementarlo con la instalación de otros en sitios específicos de la red"[33].

8.1 SANCIONES LEGALES ANTE FRAUDES INFORMÁTICOS

Debido al auge de la utilización de redes sociales, la tecnología y diversos dispositivos electrónicos, los delitos informáticos han ido en aumento hasta de un 60%

Según fuentes de la Policía Nacional "En Colombia estos delitos se pagan con multas entre los 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. Pero si los delitos son graves pueden incluir penas de prisión, que van desde los 36 a los 96 meses (ocho años) dependiendo de la gravedad del delito informático" [34]

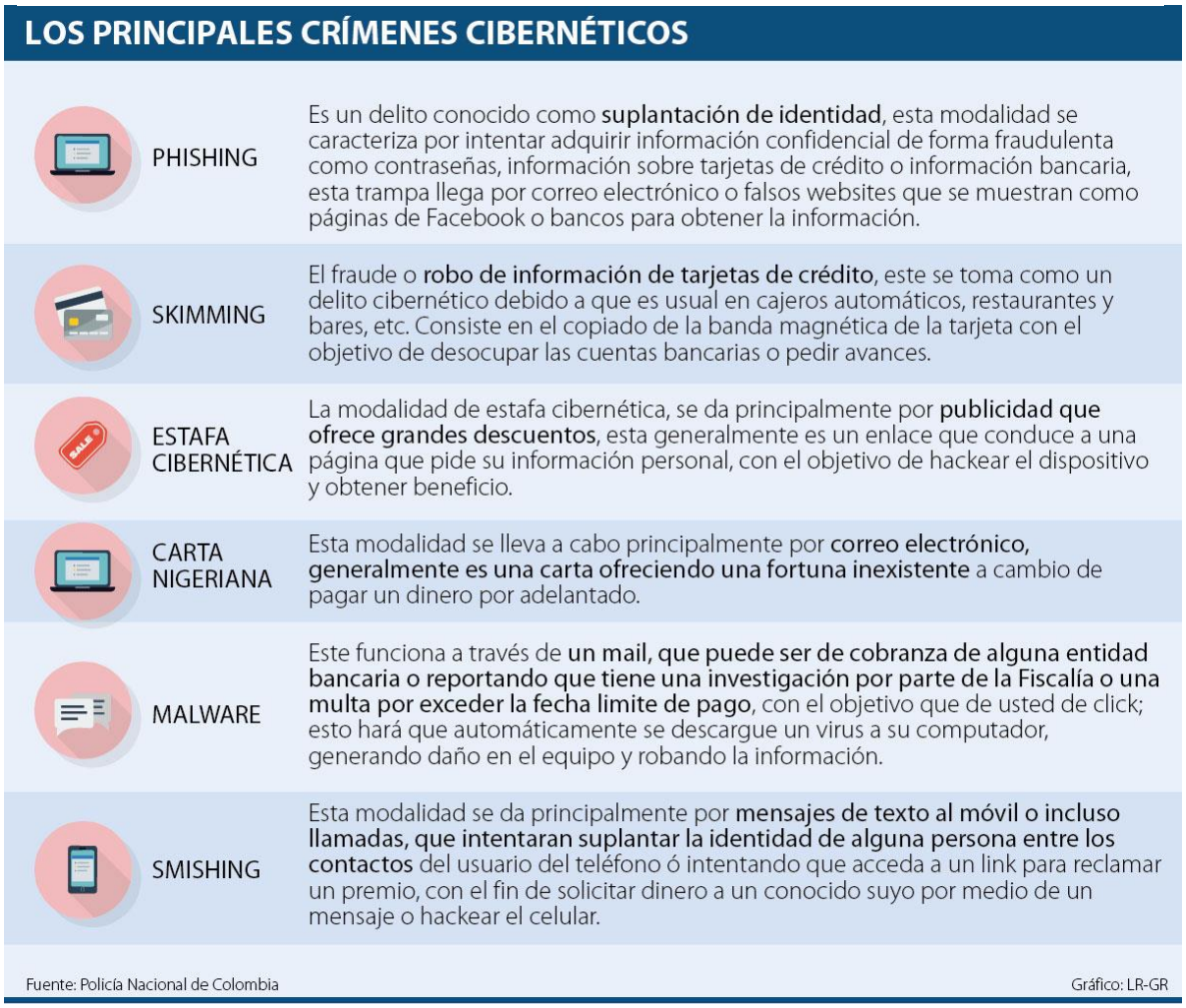
Aunque no existe en nuestro país un amplio campo de sanción ante este arquetipo de delitos, contamos con la ley 1273 de 2009 que reglamenta este tipo de infracciones informáticas. Igualmente, se conoce que el robo de cuentas bancarias es la conducta delictiva más creciente.

En la actualidad, la Policía Nacional reconoce seis principales prácticas. Actualmente, existen seis delitos cibernéticos más comunes según la Policía Nacional.

[33] PLAZAS GARCIA, Edna Rocio. Trabajo de grado: Ingeniería Social en las Empresas Colombianas [en línea]. Stadium.unad.edu.co. (2018). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

[34] PINILLA, Sebastián. Se podría pagar cárcel por ocho años por delitos cibernéticos y cuantiosas multas [en línea]. Asuntoslegales.com.co. (25 de junio de 2018). [Consultado: 6 de diciembre de 2018]. Disponible en Internet: https://www.asuntoslegales.com.co/actualidad/carcel-por-ocho-anos-por-delitos-ciberneticos-2742015

Figura 3 Delitos informáticos



Fuente: PINILLA, Sebastián. Asuntoslegales.com.co. [imagen]. Circuito de un ataque de phishing. (consultado: diciembre 6 de 2018) disponible en https://www.asuntoslegales.com.co/actualidad/carcel-por-ocho-anos-por-delitos-ciberneticos-2742015

9. RECOMENDACIONES

- Cada empresa debe tomar conciencia del riesgo que a diario tienen respecto a la seguridad de la información; por tanto, deben implementar diversos controles para proteger la misma y que posiblemente son costosas: firewalls, red de cámaras, antivirus, formación al personal, identificación biométrica y/o electrónica, etc… con lo anterior no se garantiza que no se sufrirá un ataque de ingeniería social, pero si se mitigaran los riesgos.

- La manera óptima de enfrentar los conflictos generados en la ingeniería social es formar al personal y promover medidas preventivas al respecto como: no divulgar información sensible a desconocidos, implementar políticas y controles de seguridad. Para esto se debe establecer un plan de acción riguroso y velar por su cumplimiento.

- A la hora de desechar la información que se encuentra de manera física (documentos, facturas, fichas, estratos, balances, etc.) debe garantizarse la destrucción completa del material, evitando así que caiga en manos mal intencionadas.

- De manera constante el personal encargado al interior de las organizaciones, deben hacer seguimiento a las licencias desde su caducidad.

- Garantizar que las contraseñas sean seguras y personales y que los lugares de control o centro de cómputo no sean de acceso a personal no autorizado.

- Crear políticas de seguridad de navegación para los empleados, evitando así, ingreso a páginas que nada tienen que ver con sus labores.

- Realizar constantemente backup, para evitar grandes pérdidas de información, en caso tal de presentarse un ataque de ingeniería social.

- El Administrador del Sistema, debe realizar tareas de seguimiento y control periódicos y de forma detallada a la administración remota. Debe supervisar, monitorear y vigilar los mismos para detectar intentos de inicio de sesión interactivos, además de comprobar la validez de cada intento de conexión.

10. CONCLUSIONES

- La ingeniería social inicia en un contacto casual y termina en un atentado contra la seguridad digital de una organización. Por una parte, se aprovecha de la confianza e ingenuidad de las personas para conseguir información confidencial y por otra utiliza dispositivos y/o programas informáticos con el mismo objetivo. No importa el tipo de ingeniería social utilizada, la metodología siempre es la misma.

- No importa cuánto mitiguen las altas tecnologías la vulnerabilidad presentada en la informática, ésta evoluciona a la par; por tanto, no se puede dejar de avanzar e investigar en el campo y sobre todo tener en cuenta que una de las grandes debilidades en el proceso y que permite la ingeniería social, es el sujeto, a él se le debe formar e invitar a tomar conciencia de su gran responsabilidad en las organizaciones para disminuir los riesgos. No solo se debe invertir en herramientas tecnológicas, también invertir en recursos humanos. Podría decirse que la ingeniería social es un arte que se desarrolla en las habilidades sociales de una persona en particular.

- En un mundo donde la tecnología avanza vertiginosamente ninguna organización está exenta de ser vulnerable en el tema de la seguridad. El cibercrimen afecta hoy la economía mundial; por tal motivo, pequeñas y grandes empresas deben implementar diversas políticas de seguridad y medidas de control para mitigar riesgos, aunque siempre se estará en peligro.

- Las empresas no desconocen los riesgos en cuestión de seguridad; sin embargo, limitan los recursos para la misma, pensando que nunca serán víctimas del cibercrimen.

- La ingeniería social afecta a todos, pero se encamina principalmente a las empresas y sobre todo a las del sector bancario, puesto que manejan recursos económicos. El método más utilizado es el Phishing.

BIBLIOGRAFIA

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Magerit Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I método [en línea]. Ccn-cert.cni.es. España. (Octubre de 2012). [Consultado: 23 de mayo de 2018]. Disponible en Internet: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

ARBELÁEZ, Ana. Ingeniería Social: El Hackeo Silencioso [en línea]. Enter.co. (s.f.). [Consultado: 1 de junio de 2018]. Disponible en Internet: http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/

AUTORES, V. Diccionario de internet [en línea]. Books.google.com.co. Madrid. (marzo de 2002). [Consultado: 1 de junio de 2018]. Disponible en Internet: https://books.google.com.co/books?id=aPVG77nBr80C&pg=PR9&lpg=PR9&dq=Diccionario+de+internet+complutense&source=bl&ots=OWm6diFmQ5&sig=qt7D4wDNIu9liCAB4uVQpav8eKY&hl=es&sa=X&ved=2ahUKEwi21oumjoXfAhXKxVkKHeTFC504ChDoATAAegQIBxAB#v=onepage&q=Diccionario%20de%20internet%20complutense&f=false

BERNATE, Juan Carlos. El misterioso mundo de los virus informáticos [en línea]. Revistacredencial.com. (4 de junio 2012). [Consultado: 14 de mayo de 2018]. Disponible en Internet: http://www.revistacredencial.com/credencial/noticia/tecnologia/el-misterioso-mundo-de-los-virus-informaticos

BORGHELLO, Cristian. El arma infalible: la Ingeniería Social [en línea]. Eset-la.com. (13 de abril de 2009). [Consultado: 30 de mayo de 2018]. Disponible en Internet: http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

SANDOVAL CASTELLANOS, Edgar Jair. Ingeniería Social: Corrompiendo La Mente Humana [en línea]. Revista.seguridad.unam.mx. México. (s.f.). [Consultado: 1 de junio de 2018]. Disponible en Internet: https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

FRANCO, David A.; PEREA, Jorge L. y PUELLO, Plinio. Metodología para la Detección de Vulnerabilidades en Redes de Datos [en línea]. Scielo.conicyt.cl. (2012). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014

PLAZAS GARCIA, Edna Rocio. Trabajo de grado: Ingeniería Social en las

Empresas Colombianas [en línea]. Stadium.unad.edu.co. (2018). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

REY, Jhonny. Deontología Informática [en línea]. Delitosinformatico2580.blogspot.com. (2 de noviembre de 2010). [Consultado: 30 de mayo de 2018]. Disponible en Internet: http://delitosinformatico2580.blogspot.com/

TABARES GIRALDO, Jhonathan y RODRIGUEZ ALVAREZ, Jhony Armando. Trabajo de grado: Implementación de un sistema experto para la predicción de nuevos sectores de influencia de un producto o servicio a partir de la red social twitter [en línea]. Bibliotecadigital.usb.edu.co. (2016). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://bibliotecadigital.usb.edu.co/bitstream/10819/3640/1/Implementacion_Sistema_Experto_Tabares_2016.pdf

ARIAS HIDALGO, Walter. En seguridad informática el mejor antivirus es usted[en línea]. Eafit.edu.co. (11 de noviembre de 2015). [Consultado: 30 de mayo de 2018]. Disponible en Internet: http://www.eafit.edu.co/investigacion/revistacientifica/edicion-164/Paginas/En-seguridad-inform%C3%A1tica-%E2%80%9Cel-mejor-antivirus-es-usted%E2%80%9D.aspx

INTERECONONOMÍA. Cómo prevenir un ciberataque [en línea]. Intereconomia.com. (28 de agosto de 2017). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://intereconomia.com/tecnologia/como-prevenir-un-ciberataque-20170828-1847/

JARAMILLO LONDOÑO, César. La ingeniería social un desafío investigativo [en línea]. Publicaciones.eafit.edu.co. (1996). [Consultado: 30 de mayo de 2018]. Disponible en Internet: http://publicaciones.eafit.edu.co/index.php/revista-universidad-eafit/article/view/1175/1062

KRAUSE, Mariane. La investigación cualitativa, un campo de posibilidades y desafíos [en línea]. Es.slideshare.net. (1995). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://es.slideshare.net/alejandraarrieche1/krause-m-la-investigacin-cualitativa-un-campo-de-posibilidades-y-desafos

LÓPEZ, David. La ingeniería social: el usuario continúa siendo el eslabón más débil [en línea]. Colombiadigital.net. (13 de octubre de 2015). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://colombiadigital.net/actualidad/articulos-informativos/item/8556-la-ingenieria-social-el-usuario-continua-siendo-el-eslabon-mas-debil.html

CTIC. Medidas de seguridad básicas: Los puertos de tu router [en línea]. Fundacionctic.org. (2 de mayo de 2014). [Consultado: 4 de junio de 2018]. Disponible en Internet: http://www.fundacionctic.org/sat/articulo-medidas-de-seguridad-basicas-los-puertos-de-tu-router

MITNICK, Kevin D. y SIMÓN, William L. El arte de la instrucción, cómo ser un hackers o evitarlos [en línea]. Es.slideshare.net. México. (2007). [Consultado: 4 de junio de 2018]. Disponible en Internet: https://es.slideshare.net/kissees/elartedelaintrusion-kevinmitnick

ORREGO, Jose Manuel. Ingeniería Social o simple estafa [en línea]. Revistavenamerica.com. (8 de mayo de 2017). [Consultado: 1 de junio de 2018]. Disponible en Internet: https://revistavenamerica.com/ingenieria-social-o-simple-estafa/

ZAPATA PAREJA, Carlos Andrés; CUBIDES CORRALES, Iván Dario y MURCIA GUZMAN, Maria Olga. Trabajo de Grado: Técnicas de detección y análisis de malware en entornos corporativos con sistemas operativos Windows [en línea]. Bibliotecadigital.usb.edu.co. (2015). [Consultado: 1 de junio de 2018]. Disponible en Internet: https://bibliotecadigital.usb.edu.co/bitstream/10819/4208/1/Tecnicas_Deteccion_Analisis_Zapata_2015.pdf

EL TIEMPO. Consejos para evitar ser víctima del ciberataque mundial [en línea]. Eltiempo.com. (15 de mayo de 2017). [Consultado: 1 de junio de 2018]. Disponible en Internet: https://www.eltiempo.com/tecnosfera/tutoriales-tecnologia/como-evitar-ser-victima-de-ciberataque-88120

DE SALVADOR, Luis. Ingeniería Social y Operaciones [en línea]. Ieee.es. (18 de octubre de 2011). [Consultado: 30 de mayo de 2018]. Disponible en Internet: http://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO74-2011.IngenieriaSocial_LuisdeSalvador.pdf

KASPERSKY LAB. 33 ataques por segundo: Kaspersky Lab registra un aumento del 59% en ataques de malware en América Latina [en línea]. Latam.kaspersky.com. (s.f.). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://latam.kaspersky.com/about/press-releases/2017_33-attacks-per-second-increase-in-malware-attacks-in-latin-america

RAMIREZ SANDOVAL, Jorge Iván; DÍAZ MARTÍNEZ, José Vicente y GARIZURIETA MEZA, Miguel Hugo. Ingeniería social, una amenaza informática [en línea]. Es.scribd.com. (2009). [Consultado: 2 de junio de 2018]. Disponible en Internet: https://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica

DE LA TORRE, Consuelo. Normas ISO 27001 -27002 [en línea]. Scprogress.com.

(4 de junio de 2018). [Consultado: 3 de junio de 2018]. Disponible en Internet: http://www.scprogress.com/NOTICIAS/CyberNoticia47-20170824.pdf

JAMES SCOTT, Spencer. Ingeniería Social: eludiendo el "firewall humano" [en línea]. (21 de enero de 2011). [Consultado: 3 de junio de 2018]. Disponible en Internet: http://www.magazcitum.com.mx/?p=1173#.W9e4w3tKjIU

SEMANA. El Cibercrimen en 2017: La amenaza crece sobre Colombia [en línea]. Semana.com. (28 de diciembre de 2017). [Consultado: 28 de octubre de 2018]. Disponible en Internet: https://www.semana.com/nacion/articulo/cibercrimen-en-colombia-balance-de-2017/551979

MENDOZA, Azury. Conoce los riesgos y amenazas de la Ingeniería social sobre los activos y datos sensibles [en línea]. Gb-advisors.com. (27 de febrero de 2018). [Consultado: 28 de octubre de 2018]. Disponible en Internet: http://www.gb-advisors.com/es/riesgos-y-amenazas-de-la-ingenieria-social/

DACCACH T., José Camilo. Ley de delitos informáticos en Colombia [en línea]. Deltaasesores.com. (s.f.). [Consultado: 28 de octubre de 2018]. Disponible en Internet: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

POLICIA NACIONAL. Informe: Amenazas del Cibercrimen en Colombia 2016-2017 [en línea]. Caivirtual.policia.gov.co. (marzo 2018). [Consultado: 28 de octubre de 2018]. Disponible en Internet: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

DINERO. Los sectores económicos más impactados por el cibercrimen en Colombia [en línea]. Dinero.com. (26 de septiembre de 2017). [Consultado: 2 de noviembre de 2018]. Disponible en Internet: http://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321.

RCN. Pishing, el método de robo por internet más utilizado en el país [en línea]. Noticias.canalrcn.com. (11 de octubre de 2017). [Consultado: 2 de noviembre de 2018]. Disponible en Internet: https://noticias.canalrcn.com/tecnologia-tecnologia/pishing-el-metodo-robo-internet-mas-utilizado-el-pais

JIMENEZ CANO, Rosa. Google Docs sufre un ataque de 'phishing' [en línea]. Elpais.com. (5 de mayo de 2017). [Consultado: 2 de noviembre de 2018]. Disponible en Internet: https://elpais.com/tecnologia/2017/05/04/actualidad/1493887324_006575.html.

DINERO. ¡Cuidado! Están suplantando a Bancolombia para estafar a miles de clientes [en línea]. Dinero.com. (13 de marzo de 2017). [Consultado: 4 de

noviembre de 2018]. Disponible en Internet: https://www.dinero.com/empresas/articulo/campana-de-phishing-afecta-a-miles-de-clientes-de-bancolombia/242871

RCN RADIO. Registraduría reveló que ataque informático originó fallas a la página web de la entidad [en línea]. Rcnradio.com. (28 de septiembre de 2016). [Consultado: 4 de noviembre de 2018]. Disponible en Internet: https://www.rcnradio.com/colombia/registraduria-revela-ataque-informatico-origino-fallas-la-pagina-web-la-entidad

SEMANA. No se deje engañar: estos son los correos falsos de la Fiscalía [en línea]. Semana.com. (18 de agosto de 2016). [Consultado: 5 de noviembre de 2018]. Disponible en Internet: https://www.semana.com/tecnologia/articulo/correos-falsos-de-la-fiscalia/489435

EL TIEMPO. Alerta por correos falsos que atacan a usuarios de MasterCard y Visa [en línea]. Eltiempo.com. (29 de marzo de 2016). [Consultado: 5 de noviembre de 2018]. Disponible en Internet: http://www.eltiempo.com/archivo/documento/CMS-16549207

RPP NOTICIAS. Bitcoin, la moneda virtual que exigen los hackers tras el ciberataque [en línea]. Rpp.pe. (12 de mayo de 2017). [Consultado: 6 de noviembre de 2018]. Disponible en Internet: http://rpp.pe/economia/economia/bitcoin-la-moneda-en-que-piden-rescate-los-hakers-del-ciberataque-mundial-noticia-1050368

HERALDO. ¿Por qué los hackers del ciberataque global exigen los rescates en bitcoins? [en línea]. Heraldo.es. (16 de mayo de 2017). [Consultado: 6 de noviembre de 2018]. Disponible en Internet: http://www.heraldo.es/noticias/sociedad/2017/05/16/por-que-bitcoins-1175631-310.html

ESCUDERO RUBIO, Víctor; MARQUEZ SOLIS, Santiago y PREUKSCHAT, Alex. Ciberseguridad cinco claves sobre bitcoin y el ataque informático mundial [en línea]. Retina.elpais.com. (14 de mayo de 2017). [Consultado: 6 de noviembre de 2018]. Disponible en Internet: https://retina.elpais.com/retina/2017/05/12/tendencias/1494619771_719922.html

IGLESIAS, Pablo F. #Mundo Hacker: Los 6 principios básicos de la ingeniería social [en línea]. Pabloyglesias.com. (s.f.). [Consultado: 18 de noviembre de 2018]. Disponible en Internet: https://www.pabloyglesias.com/mundohacker-ingenieria-social/

PISCITELLI, Emiliano. Ingeniería Social: Cuáles son los tipos de ataque [en línea]. Redusers.com. (4 de diciembre de 2015). [Consultado: 18 de noviembre de 2018].

Disponible en Internet: http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/

PINILLA, Sebastián. Se podría pagar cárcel por ocho años por delitos cibernéticos y cuantiosas multas [en línea]. Asuntoslegales.com.co. (25 de junio de 2018). [Consultado: 6 de diciembre de 2018]. Disponible en Internet: https://www.asuntoslegales.com.co/actualidad/carcel-por-ocho-anos-por-delitos-ciberneticos-2742015

ANEXOS

Anexo A Formato RAE

Fecha de Realización: 11/12/2018
Título: Estudio Monográfico: Ingeniera social como delito informático en las grandes empresas colombianas.
Autor: NOVOA GUTIERREZ, Edwin Alberto
Palabras Claves: Ingeniería Social, Técnicas, Vulnerabilidades, Seguridad Informática, Ataques, Delitos, Phishing, Categorías, Bitcoins, cibercrimen, empresas.
Descripción: Trabajo Monográfico para optar por el título de Especialista en Seguridad Informática de la Universidad Nacional Abierta y a Distancia.
Fuentes: 42 fuentes bibliográficas. MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. Magerit Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I método [en línea]. Ccn-cert.cni.es. España. (Octubre de 2012). [Consultado: 23 de mayo de 2018]. Disponible en Internet: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html ARBELÁEZ, Ana. Ingeniería Social: El Hackeo Silencioso [en línea]. Enter.co. (s.f.). [Consultado: 1 de junio de 2018]. Disponible en Internet: http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/ AUTORES, V. Diccionario de internet [en línea]. Books.google.com.co. Madrid. (marzo de 2002). [Consultado: 1 de junio de 2018]. Disponible en Internet: https://books.google.com.co/books?id=aPVG77nBr80C&pg=PR9&lpg=PR9&dq=Diccionario+de+internet+complutense&source=bl&ots=OWm6diFmQ5&sig=qt7D4wDNIu9liCAB4uVQpav8eKY&hl=es&sa=X&ved=2ahUKEwi21oumjoXfAhXKxVkKHeTFC504ChDoATAAegQIBxAB#v=onepage&q=Diccionario%20de%20internet%20complutense&f=false BERNATE, Juan Carlos. El misterioso mundo de los virus informáticos [en línea]. Revistacredencial.com. (4 de junio 2012). [Consultado: 14 de mayo de 2018]. Disponible en Internet: http://www.revistacredencial.com/credencial/noticia/tecnologia/el-misterioso-

mundo-de-los-virus-informaticos
BORGHELLO, Cristian. El arma infalible: la Ingeniería Social [en línea]. Eset-la.com. (13 de abril de 2009). [Consultado: 30 de mayo de 2018]. Disponible en Internet: http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

SANDOVAL CASTELLANOS, Edgar Jair. Ingeniería Social: Corrompiendo La Mente Humana [en línea]. Revista.seguridad.unam.mx. México. (s.f.). [Consultado: 1 de junio de 2018]. Disponible en Internet: https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

FRANCO, David A.; PEREA, Jorge L. y PUELLO, Plinio. Metodología para la Detección de Vulnerabilidades en Redes de Datos [en línea]. Scielo.conicyt.cl. (2012). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://scielo.conicyt.cl/scielo.php?script=sci_arttext&pid=S0718-07642012000300014

PLAZAS GARCIA, Edna Rocio. Trabajo de grado: Ingeniería Social en las Empresas Colombianas [en línea]. Stadium.unad.edu.co. (2018). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

REY, Jhonny. Deontología Informática [en línea]. Delitosinformatico2580.blogspot.com. (2 de noviembre de 2010). [Consultado: 30 de mayo de 2018]. Disponible en Internet: http://delitosinformatico2580.blogspot.com/

TABARES GIRALDO, Jhonathan y RODRIGUEZ ALVAREZ, Jhony Armando. Trabajo de grado: Implementación de un sistema experto para la predicción de nuevos sectores de influencia de un producto o servicio a partir de la red social twitter [en línea]. Bibliotecadigital.usb.edu.co. (2016). [Consultado: 30 de mayo de 2018]. Disponible en Internet: https://bibliotecadigital.usb.edu.co/bitstream/10819/3640/1/Implementacion_Sistema_Experto_Tabares_2016.pdf

ARIAS HIDALGO, Walter. En seguridad informática el mejor antivirus es usted[en línea]. Eafit.edu.co. (11 de noviembre de 2015). [Consultado: 30 de mayo de 2018]. Disponible en Internet: http://www.eafit.edu.co/investigacion/revistacientifica/edicion-164/Paginas/En-seguridad-inform%C3%A1tica-%E2%80%9Cel-mejor-antivirus-es-usted%E2%80%9D.aspx

Contenido del documento: Hablar hoy de ingeniería social es más frecuente de

lo que parece, pues surge como todo un proceso dedicado a intervenir en las actitudes, relaciones y acciones de la humanidad. Esta afecta a todos en la sociedad, pero se enfoca principalmente a las empresas u organizaciones que manejan gran tipo de información; las organizaciones más sensibles a un ataque de ingeniería social son las del sector bancario, puesto que manejan recursos económicos. El método más utilizado es el Phishing.

El presente trabajo tiene como objetivo conocer en qué consiste la ingeniería social, cómo afecta a las grandes empresas colombianas sobre todo a las distribuidoras de productos de alto consumo y rotación y cuáles son las medidas que estas toman para mitigar los riesgos ante la misma.

Para llevar a cabo el presente trabajo se ha partido de la importancia que ha tomado la tecnología y la informática en todos los procesos de la sociedad y la influencia que esta puede llegar a tener en la vida de las personas. Se citan casos presentados en algunas empresas colombianas, se desglosan los tipos de ingeniería utilizados desde las personas y desde la web, las metodologías y se hacen algunas recomendaciones para afrontar los conflictos que se presentan en relación con el cibercrimen.

Igualmente, se busca dejar claro que para llevar a cabo un ataque de ingeniería social, no es necesario tener conocimientos técnicos o formación en el campo, basta con contar con buenas habilidades sociales y malas intenciones para acceder a la información sensible, pero crucial de cualquier organización.

La investigación se desarrolla desde las siguientes categorías: ingeniería social, comunicación, sistema, seguridad y confianza. En la referencia teórica se hace lectura de autores como Ana Arbeláez, Edgar Castellanos y Jair Sandoval, Cristian Borghello, David Franco, Walter hidalgo, César Jaramillo, David López y José Manuel Orrego.

Hoy hablar de ciber seguridad es vital, la sociedad se encuentra en un momento donde la tecnología es el auge del desarrollo y el internet transversaliza el mismo.

Por naturaleza el ser humano tiende a proteger lo que considera suyo y confía en que personas, espacios o lugares en donde entrega su información le brinde seguridad y confianza ante la misma.

Las empresas colombianas poseen gran información de la población y están constantemente vulnerables a ataques. Las mismas, asiduamente plantean nuevas estrategias: antivirus, sistemas de bloqueos, detención, etc… sin embargo, no desconocen que hay otro tipo de manipulación de la tendencia humana para usar la información sensible y es la *Ingeniería Social, ésta en* lugar de lidiar con las complejas protecciones instaladas, engañan a los miembros de la

organización. Por eso se hace urgente una debida información y formación al respecto.

El presente trabajo busca presentar las Técnicas de Ingeniería Social a las que son vulnerables las Grandes Empresas Colombianas y como se pueden prevenir, muchas de los cuales, han existido hace tiempo y otras que han surgido y tienen gran éxito.

Se hace importante interpretar o visualizar de otra manera la realidad circundante de las organizaciones y/o empresas colombianas. Hoy es inevitable hablar de la importancia que ha tomado la tecnología y la informática en todos los procesos para las diversas organizaciones. El mundo organizacional tiene una gran obligación entre y para la sociedad, éste cada día almacena grandes cantidades de información y la misma es importante en diversos grados; sin embargo y ante el vertiginosos cambio, se hace urgente posibilitar la protección de la misma sin importar como se recolecte: física o digital; llámese ésta protección en el ámbito empresarial, hacer uso de salvaguardas. Cabe recordar que la información es el eje central de la organización y esta recolecta, datos financieros, personales, comerciales, técnicos, entre otros. Teniendo en cuenta lo anterior se hace necesario conocer los riesgos y plantear nuevas estrategias de seguridad en las organizaciones, puesto que son muy vulnerables a la perdida, robo o secuestro de la Información.

Es necesario tener en cuenta que a medida que se posibilitan herramientas y aplicaciones que hacen más ágil el trabajo y lo facilitan más organizado, también surgen otras que amenazan la seguridad y buscan ser obstáculo en el proceso; es aquí, donde aparecen personas mal intencionadas con programas que ciber atacan la información, éstas conocidas como Hackers, Copyhackers y los Phreak, todos caracterizados por poseer altos conocimientos en el área de la tecnología.

Por otro lado, si una empresa quiere ser competitiva en la actualidad debe contar con sistemas y plataformas súper ágiles y seguras y esto conlleva un cambio en el proceso de transformación digital. Pero de nada sirve tener los mejores sistemas de protección, sino se cuenta con personal idóneo y seguro de su labor, personas con astucia y formación para sospechar ante la presencia de terceros sin escrúpulos que solo buscan perjudicar la organización como tal. Los ciber delincuentes están listos a aprovechar cualquier oportunidad que se les presente para agredir y cada día la *Ingeniería Social* es más utilizada para este tipo de ataques. Por tanto, es necesario que las empresas le den la importancia que se merece la *Protección de la Información* y sensibilice a todo su personal de la gran responsabilidad que se tiene y tome conciencia de que la seguridad se fundamente en la confianza. Dado todo lo anterior, este trabajo busca responder la siguiente cuestión ¿Qué estrategias se deben implementar en las empresas colombianas distribuidoras de productos de alto consumo y rotación; para prevenir y/o disminuir

el riesgo de ataques de ingeniería social?

Metodología: Por las características del documento, no presenta.

Conclusiones: La ingeniería social inicia en un contacto casual y termina en un atentado contra la seguridad digital de una organización. Por una parte se aprovecha de la confianza e ingenuidad de las personas para conseguir información confidencial y por otra utiliza dispositivos y/o programas informáticos con el mismo objetivo. No importa el tipo de ingeniería social utilizada, la metodología siempre es la misma.

No importa cuánto mitiguen las altas tecnologías la vulnerabilidad presentada en la informática, ésta evoluciona a la par; por tanto, no se puede dejar de avanzar e investigar en el campo y sobre todo tener en cuenta que una de las grandes debilidades en el proceso y que permite la ingeniería social, es el sujeto, a él se le debe formar e invitar a tomar conciencia de su gran responsabilidad en las organizaciones para disminuir los riesgos. No solo se debe invertir en herramientas tecnológicas, también invertir en recursos humanos. Podría decirse que la ingeniería social es un arte que se desarrolla en las habilidades sociales de una persona en particular.

En un mundo donde la tecnología avanza vertiginosamente ninguna organización está exenta de ser vulnerable en el tema de la seguridad. El cibercrimen afecta hoy la economía mundial; por tal motivo, pequeñas y grandes empresas deben implementar diversas políticas de seguridad y medidas de control para mitigar riesgos aunque siempre se estará en peligro.

Las empresas no desconocen los riesgos en cuestión de seguridad; sin embargo, limitan los recursos para la misma, pensando que nunca serán víctimas del cibercrimen.

La ingeniería social afecta a todos, pero se encamina principalmente a las empresas y sobre todo a las del sector bancario, puesto que manejan recursos económicos. El método más utilizado es el Phishing.

AUTOR: EDWIN ALBERTO NOVOA GUTIERREZ