INGENIERIA SOCIAL EN LAS EMPRESAS COLOMBIANAS

ING. EDNA ROCIO PLAZAS GARCIA

Monografía de investigación para optar al título de Especialista en Seguridad Informática

Director

Luis Fernando Zambrano Hernández

Ingeniero

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
PITALITO – HUILA
2018

Nota de aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del presidente del jurado

_____
Firma del jurado

_____
Firma del jurado

Pitalito 02 de mayo de 2018

DEDICATORIA

Aprovecho esta oportunidad para de dedicar este nuevo triunfo en mi vida, a Dios por toda su generosidad y por ser el artífice de todo lo que logramos ver y sentir, por brindarme una hermosa familia que me da su apoyo en cada proyecto que emprendo, por darme siempre su dirección perfecta.

A mi novio por su cariño, compresión y sacrificio; a mis padres y mis hermanos quienes con su apoyo incondicional y su motivación me ayudaron a alcanzar este nuevo peldaño en mi vida.

AGRADECIMIENTOS

Al culminar una meta profesional tan importante, es necesario reconocer gratamente a cada uno de los pilares de mi vida, quienes hicieron de este sueño una realidad.

A Dios, gracias por ser el creador de la vida, quien me ha dotado de capacidad, inteligencia y perseverancia, para lograr este tan importante título. Por siempre guiarme en los pasos que doy día a día.

A mí Madre quien ha sido mi apoyo incondicional, económica y moralmente y ha estado ahí, apoyándome en cada paso que doy durante toda mi vida, desde que nací hasta hoy en día, y le agradezco porque siempre me ha dado ánimos de seguir adelante.

A mi Padre por ser un ejemplo para mí, por ayudarme y apoyarme cuando lo he necesitado, por sus consejos acertados en todo momento.

A mis hermanos, gracias por el apoyo y el amor incondicional que me brindan y por alentarme a seguir adelante con mis proyectos de vida.
Gracias Familia porque es a ustedes a quienes debo el éxito que hoy he alcanzado.

A la Universidad Nacional Abierta y a Distancia UNAD, gracias por recibirme y permitirme culminar este ciclo, al programa de Especialización en seguridad informática, por facilitarme muchos de los recursos necesarios para el desarrollo del mismo, al director de trabajo de grado el Ingeniero Fernando Zambrano, gracias por su gran disponibilidad, atención y paciencia al escuchar cada idea, cada inconveniente, cada acierto, de las diferentes etapas del desarrollo del trabajo de grado.

Gracias a mis amigos y compañeros que me brindaron una voz de aliento para seguir adelante con este proyecto, gracias por sus consejos y entrega en los momentos que los necesité.

Muchas gracias a todos, este logro, es el comienzo del camino de mis sueños por cumplir.

CONTENIDO

Pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE GRAFICAS

Pág.

INTRODUCCION

Permanentemente se escucha en los medios de comunicación robos a entidades bancarias vía internet y son miles de personas las afectadas, ya que los ahorros de toda su vida desaparecen sin ninguna explicación; es de ahí donde surge la pregunta ¿cómo lo hicieron? La ingeniería social es parte de la respuesta, debemos de tener en cuenta que esta no solo es aplicada por los delincuentes informáticos, también es utilizada por los ladrones, los cuales averiguan el nombre de los ocupantes de una casa y vigilan sus actividades diarias.

Con este trabajo se quiere lograr que una vez finalizado su análisis, el lector tenga en claro el concepto de Ingeniería Social, su objetivo, quiénes lo utilizan y quiénes son los más vulnerables.

Para ello, se introducirán algunos conceptos a nivel general de Ingeniería Social, luego se citarán algunos de los casos ocurridos en empresas colombianas, igualmente se realizará un análisis de las diversas técnicas de ingeniería social que año tras año han evolucionado en Colombia y por último se pretende fomentar los buenos hábitos de seguridad informática, para disminuir los ataques de ingeniería social en las empresas colombianas.

1. FORMULACIÓN DEL PROBLEMA

La información que se encuentra acerca de la ingeniería social en Colombia en los diferentes sitios web es muy limitada, ya que algunas empresas para no generar alarmas no publican y manejan un perfil bajo para estas situaciones.

Las empresas no quieren asesorarse sobre la ingeniera social porque es un gasto más para sus corporaciones, pero esto podría afectar la información de sus clientes, los cuales al no estar asesorados por las empresas pueden llegar a caer en algún tipo de técnica empleada por los delincuentes para robar, suplantar sus datos, así mismo afectar la seguridad de sus sistemas de información. Esto ha llevado a especialistas de seguridad informática a estar atentos a nuevos mecanismos de seguridad informática, para alertar a los usuarios, tanto como a las empresas como a los clientes que frecuentan dichas empresas, permitiendo un nivel de seguridad aceptable.

¿Qué hábitos de seguridad, se deben fomentar en las empresas colombianas para disminuir los ataques de ingeniería social?

2. JUSTIFICACIÓN

La ingeniería social ha sido usada no solamente para vulnerar sistemas informáticos de las diferentes empresas existentes en el mundo, si no también ha sido útil para ganar guerras; un ejemplo de estos ataques de ingeniería social se hizo en la ciudad de Troya, cuyas murallas eran consideradas inaccesibles. Según cuenta la historia No existía arma ni ejército capaz de romper las murallas de Troya, sin embargo, los griegos utilizaron su astucia y construyeron un enorme caballo de madera que en su interior aguardaba un ejército, este caballo lo obsequiaron y con el lograron tomarse la famosa ciudad de Troya. En este ejemplo se puede apreciar que los griegos obraron con astucia y lograron conquistar lo imposible por medio del ingenio y la manipulación. Los ataques por internet han ido evolucionado año tras año; ahora, los delincuentes informáticos no buscan conseguir entrar a la cuenta de correo electrónico de una persona para robar información, más bien intentan ganar la confianza de los usuarios a través de engaños y con esto lograr estafarlos.

La Ingeniería social es una técnica que pueden usar ciertas personas tales como investigadores privados o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información, que les permitan realizar algún acto que perjudique o exponga los datos de la persona u empresa comprometiéndolo a riesgos o abusos. La mayoría de los bancos que hay en territorio colombiano, están bajo presión para aumentar la seguridad, ya que tendencias como la creciente adopción de la banca móvil ponen las defensas de la infraestructura TI en mayor riesgo de sufrir ataques cibernéticos.

Por el motivo expuesto anteriormente este trabajo de grado servirá para mostrar las diversas técnicas que utilizan los delincuentes informáticos para aplicar ingeniería

social a sus víctimas, como identificarlos y como evitarlos a través de los buenos hábitos de seguridad informática en Colombia.

3. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Se tomará el sector de las empresas colombianas y se dará a conocer cuáles son los ataques más utilizados en ingeniería social, como identificarlos y como evitarlos a través de los buenos hábitos de seguridad informática.

4. OBJETIVOS DE PROYECTO

4.1 OBJETIVO GENERAL

Demostrar por medio de un análisis bibliográfico la evolución e innovación de los ataques de ingeniería social que se han realizado en los últimos años a las empresas colombianas.

4.2 OBJETIVOS ESPECIFICOS

- Realizar el estudio teórico acerca de los ataques de ingeniería social que se han perpetrado a las empresas colombianas.

- Hacer un análisis que permita tener claro el concepto de Ingeniería Social, su objetivo, quiénes lo utilizan, quiénes son los más vulnerables y cuáles son los ataques de ingeniería social que se han realizado en los últimos años a las empresas colombianas.

- Hacer recomendaciones donde se fomente los buenos hábitos de seguridad, para disminuir los ataques de ingeniería social en las empresas colombianas.

5. MARCO DE REFERENCIA

En el año de 1989 se presentó “el primer ataque informático de la historia, cuando una empresa de venta de revistas estaba promocionando disquetes, para llamar la atención de los transeúntes, esta empresa regalaba a disquetes a todos los que pasaran por enfrente de la empresa, al hacer ingresarlos a los computadores, los ciudadanos se dieron cuenta que estos estaban infectados por un malware”[1].

En ese mismo año, “la empresa IBM comercializo el primer programa antivirus en el mercado”[2], lo que dio origen a grandes ganancias en el mercado de la protección de la información de los usuarios informáticos.

Actualmente existen diferentes maneras de ejecutar ataques informáticos a través de modalidades efectivas y en donde los ciber-delincuentes hacen caer a sus víctimas. En cuanto a este tema existen varios trabajos de investigación realizados en todo el mundo, se pueden mencionar algunos de ellos, por ejemplo:

En cuanto a antecedentes, a nivel de la UNAD, solo existe un trabajo relacionado con la ingeniería social. Este proyecto lo hizo un estudiante de la ciudad de Neiva Huila, perteneciente al programa de Especialización en seguridad informática, este trabajo era de modalidad investigativa, referente al tema de la seguridad de la información en la Universidad Cooperativa de Colombia, enfocado en las vulnerabilidades utilizadas por la Ingeniería Social.

---

[1] RAMÍREZ SANDOVAL, Jorge Iván; DÍAZ MARTÍNEZ, José Vicente y GARIZURIETA MEZA, Miguel Hugo. “Ingeniería Social, una amenaza informática”. Scrib [en línea], septiembre 2009 [citado en 20 noviembre de 2017]. Disponible en Internet: http://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica>.

[2] FICARRA, Francisco. “Los virus informáticos: Entre el negocio y el temor”. Revista Latinoamericana de Comunicación CHASQUI [en línea], junio 2002 [citado en 20 de noviembre de 2017]. Disponible en Internet: <http://www.redalyc.org/articulo.oa?id=16007810>. ISSN 1390-1079.

A nivel general, en otras universidades del mundo, encontramos trabajos de grado de ingeniería social, como, por ejemplo:

- Un trabajo de grado realizado en el año 2011, acerca de la "psicología aplicada a la seguridad informática"[3], en este informe se habla sobre las técnicas o manuales que se utilizan en los ataques de ingeniería social en los sistemas informáticos de las grandes plataformas de Internet.

- Otro trabajo de grado realizado en el año 2012, sobre el "impacto de la técnica del phishing en la ingeniería social"[4], esta investigación presenta un panorama actual del problema del Phishing e informa cual es la legislación referente a la protección de datos personales del gobierno Mexicano.

5.1 MARCO TEORICO

"La Seguridad de la Información se puede definir como un conjunto de medidas técnicas, organizativas y legales que permiten a las organizaciones asegurar la confidencialidad, integridad y disponibilidad de su sistema de información."[5]

---

[3] ARCOS, Sergio. 2011. "Tesís Ingeniería social: Psicología aplicada a la seguridad informática". Madrid: s.n., 2011. [Citado en 20 de noviembre de 2017]. Disponible en Internet: http://upcommons.upc.edu/bitstream/handle/2099.1/12289/73827.pdf?sequence=1

[4] GONZALEZ JUAREZ & PEÑA ENRIQUEZ, Diego Dante & José Antonio. 2012. "*ESTUDIO DEL IMPACTO DE LA INGENIERÍA SOCIAL – PHISHING".* Mexico, Scrib [en línea] 2012. [Citado en 20 noviembre de 2017]. Disponible en Internet: http://www.ptolomeo.unam.mx:8080/xmlui/bitstream/handle/132.248.52.100/2730/Tesis.pdf?sequence=1

[5] MIFSUD, Elvira. "Introducción a la seguridad informática" [en línea]. [Madrid, España]: Observatorio Tecnológico, marzo 2012 [citado en 20 noviembre de 2017]. Disponible en Internet: http://recursostic.educacion.es/observatorio/web/ca/software/software-general/1040-introduccion-a-la-seguridad-informatica?start=1.

Mientras que “la seguridad informática consiste en la implantación de un conjunto de medidas técnicas destinadas a preservar la confidencialidad, la integridad y la disponibilidad de la información, pudiendo, además, abarcar otras propiedades, como la autenticidad, la responsabilidad y la fiabilidad”[6].

En un informe encontrado en la red, denominado “Encuesta Global 2008 de Seguridad & Privacidad”, se revela la noticia de que los bancos que tienen sedes en territorio Colombiano, denunciaron un incremento importante de los delitos informáticos relacionados con la banca en línea. Según el análisis realizado a la información suministrada en ese informe se puede deducir que, desde la fecha en que se hizo el informe hasta el día de hoy, este tipo de ataques pudo aumentar, teniendo en cuenta el uso masivo de dispositivos móviles y la consolidación del comercio electrónico en Colombia.

La ingeniería social hace referencia a la capacidad que tiene una persona para influir en la conducta de un grupo de personas. En el contexto de la informática, la ingeniería social son las técnicas utilizadas por delincuentes cibernéticos para engañar a los usuarios a fin de que realicen acciones específicas o revelen información confidencial de ellos o de las empresas donde laboran, para que estos ladrones puedan beneficiarse.

[6] Ibid., p. 2.

Figura. 1 Caricatura de un ataque de Ingeniería Social

Fuente: http://www.cristiancisternas.com/2016/01/ingenieria-social-labs.html

La Ingeniería Social, en pocas palabras es una manera no convencional de obtener información deseada de manera sutil, rápida y segura de parte de las personas. Está es basada en el engaño y la manipulación de usuarios para obtener información confidencial de empresas o individuos.

La ingeniería social ha evolucionado mucho en el área de la seguridad informática y se ha vuelto la herramienta principal de los delincuentes informáticos, ya que estos se aprovechan de las debilidades tecnológicas de los seres humanos.

Existen muchas formas de hacer un ataque de Ingeniería Social, por ejemplo: Un atacante puede llamar a una casa o empresa e imitar la voz de un funcionario de alguna empresa y obtener información confidencial que luego le permita obtener acceso no autorizado a cuentas bancarias, correos electrónicos, redes sociales, etc. Otra forma puede ser por medio del internet, cuando nos salen avisos de que hemos ganado algo, o avisos para mirar videos prohibidos de algún personaje famoso, las personas por curiosidad cometemos el error de dar clic en esos avisos y cuando

entramos nos piden unos datos como nombres de usuario y contraseña, lamentablemente la mayoría de la gente pone la misma contraseña que utilizan en otras redes y estos delincuentes aprovechan que ya obtienen un password para acceder a múltiples sitios bajo la identidad de su víctima.

Otro ejemplo de la forma como los ladrones informáticos conocen información de sus víctimas es por medio del espionaje atreves de la basura; este método consiste en encontrar información entre las canecas de basura de una oficina o casa. Entre la basura pueden encontrarse números telefónicos, organigramas, manuales de las políticas de la compañía, manuales de sistemas, planos de las instalaciones, CDs, DVDs, agendas personales, etc. Toda esta "basura" puede ser una gran fuente de información para el atacante, ya que por lo menos en las agendas telefónicas se puede encontrar nombres y números de teléfono de posibles víctimas. “Los organigramas pueden revelar quienes están en cargos importantes. Los manuales de políticas pueden servir para saber qué tan segura es esa empresa. Los calendarios pueden indicar que empleado va a estar fuera de la oficina cierto día”[7], etc.

El método más avanzado para obtener acceso no autorizado a un sistema informático o información por parte de los ciber-delincuentes es conocido como "Ingeniería Social Inversa". Este método consiste en que el atacante suplanta a una persona que se encuentra en una posición de alto rango en una empresa, este atacante tiene como característica principal la autoridad con la que trata a los empleados de dicha empresa, haciendo que estos le presenten informes a él, sin hacerle ninguna pregunta.

[7] CASTELLANOS, Luis. “*Ingenieria social siglo XXI”.* 2009. Scrib [en línea]. [Citado en 20 noviembre de 2017]. Disponible en Internet: https://ingenieriasocialsigloxxi.wordpress.com/2009/11/03/revision-de-desperdicios-o-basura/

Si se investiga, planea y ejecuta adecuadamente, este ataque puede brindarle al atacante mayores oportunidades de obtener información valiosa de los propios empleados; sin embargo, este ataque requiere de un alto grado de preparación e investigación para tener éxito.

Las personas que manejan la ingeniería social utilizan métodos básicos de persuasión como la suplantación para hacer robos de información de sus víctimas. Sin importar el método que se maneje, el objetivo es convencer a la víctima de que el atacante es en realidad una persona a quien confiarle información sensible. Algo que tienen muy claro los ciber-delincuentes es que ellos no buscan obtener toda la información en un solo ataque, para no ser descubiertos, pero si conseguirla toda en varios ataques en diferentes ocasiones.

La Ingeniería social suele enfocarse en el recurso humano de las empresas, donde hay diferentes tipos de personas. Por lo general la mayoría de los empleados pretenden siempre quedar bien y por tal razón, brindan información sensible sin ninguna restricción a quien la solicite. También hay empleados con pocos conocimientos en informática o que ignoran la existencia de los diferentes tipos de amenazas informáticas. En las organizaciones también fallan al no implementar, controles básicos de seguridad informática que apoyen los procesos de protección de la información. La razón principal por la que esto no se hace, es porque las directivas creen que la prevención de dichos incidentes de seguridad es demasiado costosa.

Como contramedida, la única manera de reducir el aumento de ataques de Ingeniería Social es por medio de la educación. Absolutamente todas las personas que forman parte de la organización, desde la secretaria, el personal encargado de la limpieza, los encargados de la parte administrativa, los de los altos cargos, etc.

Deben ser capacitados en cuanto a las debilidades y los métodos de engaño más empleados por los atacantes informáticos para que logren identificarlos y dar aviso de cualquier anomalía que se produzca al personal encargado.

La formación en técnicas de seguridad informática debe iniciar en el personal encargado del sector TI de la empresa, quienes son los responsables de trasmitir los conocimientos adquiridos al resto de trabajadores a través de capacitaciones como parte de sus planes de acción y con esto reducir un poco la amenaza de ataques de ingeniería social. Si las empresas capacitan a los empleados de sistemas y estos a su vez al resto de empleados, se disminuyen los recursos a invertir en temas de seguridad, ya que los incidentes tenderían a desaparecer, al menos, en lo que a Ingeniería Social se refiere.

Todos los ataques informáticos cuentan con una metodología básica donde se enmarcan todos y cada uno de los movimientos necesarios para cumplir el objetivo. Todo depende de las pretensiones del agresor y de las barreras de seguridad con que cuenta el objetivo. Al final, la metodología siempre es la misma.
La ingeniería social no es la excepción, para poder ejecutar un ataque mediante alguno de sus métodos, se deben tener en cuenta los siguientes 6 pasos:

Figura. 2 Pasos para la ejecución de ataques basados en Ingeniería Social

Fuente:Http://www.slideshare.net/acurbelo/ingenieria-social-el-lado-humano-del-hacking

A continuación, se detalla cada uno de los pasos indicados en la imagen anterior.

Paso 1. Identificar a la víctima: Aquí el atacante se plantea el objetivo y estima las probabilidades de éxito que tendría al realizar el ataque. El blanco puede ser una persona o una organización. Esta es la actividad inicial antes de ejecutar el ataque de ingeniería social.

Paso 2. Reconocimiento: Luego de establecer quien va ser su víctima, el ciber atacante inicia la búsqueda de datos sobre su objetivo que le puedan servir para su ataque. Puede obtener información disponible en directorios telefónicos, redes sociales, también buscar información en la basura de su víctima, tratar de desarrollar confianza o hacer "*phishing*".

Paso 3. Crear el escenario: La configuración del escenario del ataque, depende del ingenio del atacante, de la seguridad existente con la que cuente la víctima y de las instalaciones físicas de la empresa donde quiere ingresar. Con un poco de

suerte y gracias a las fallas en los controles de seguridad de las empresas estos delincuentes podrían hallar el escenario perfecto para actuar.

Paso 4. Realizar el ataque: El atacante pone en práctica técnicas como la Ingeniería Social Inversa, el uso de software como "*sniffers*" y "*keyloggers*", el escaneo de puertos y los mapeos de red, el *phishing* o lo más fácil hacerse amigo de la víctima y ganarse su confianza.

Paso 5. Obtener la información: Con el control de la situación, de la red, o de la computadora, el ingeniero social procede a captar la información que necesita, ya sea en un medio portátil de almacenamiento como una memoria UBS, smartphone y/o cámara digital, o simplemente hace uso de "*malware*" que envíe constantemente los datos a una dirección de correo electrónico preestablecida.

Paso 6. Salir: Cumplido el objetivo del ataque por parte del ingeniero social, este debe abandonar el lugar o la situación sin levantar sospecha alguna, manteniendo la calma y el rol asumido desde el principio.

Vale la pena resaltar que el poder identificar cada una de las etapas que conforman un ataque de Ingeniería Social "brinda la ventaja de aprender a pensar como los atacantes y a jamás subestimar su mentalidad. Desde la perspectiva del profesional en seguridad, se debe aprovechar esas habilidades para comprender y analizar la forma en que los atacantes llevan a cabo un ataque"[8].

[8] MIERES, Jorge. Enero 2009. "Ataques informáticos: Debilidades de seguridad comúnmente explotadas". {En línea}. [Citado en 20 noviembre de 2017]. Disponible en: (https://www.evilfingers.net/publications/white_AR/01_Ataques_informaticos.pdf).

5.2 MARCO CONCEPTUAL

Confidencialidad: Es la característica que posee un archivo, en la cual este sólo es leído por la persona autorizada.

Integridad: Un archivo al no haber sido alterado y no haber sido manipulado se considera que es un documento integro.

Fiabilidad: Es la probabilidad de que un sistema operativo no presente fallas, ósea que funcione con normalidad.

Autorización: Proceso mediante el cual una empresa X o persona, otorga permisos a una persona o programa informático para que este pueda ejecutar una tarea específica.

Phishing: Método de ingeniería social, que consiste en enviar correos electrónicos falsos a las cuentas de sus víctimas, en donde se les solicita que se registren o que accedan a un sitio web suplantado para luego ellos obtener sus datos de acceso.

Hackers: Los hackers son individuos que utilizan técnicas de penetración para acceder al sistema informático de alguna compañía o de alguna persona, para obtener datos que solo les beneficie a ellos. Estos son expertos en lenguajes de programación, arquitecturas de red y protocolos de comunicaciones, sistemas operativos, según los hackers, ellos no pretenden causar daño a los sistemas que atacan, sino, mejorar sus conocimientos y ayudar a descubrir vulnerabilidades en dichos sistemas para luego corregirlas.

Crackers: Se llama así a las personas encargadas de dañar los sistemas de seguridad de software licenciado, para su uso no autorizado.

Phreakers: Son los individuos que utilizan su conocimiento sobre el funcionamiento de teléfonos y celulares, pudiendo obtener llamadas gratis y beneficios del sector de telefonía gracias a sus técnicas o métodos utilizados.

Spammers: Los spammers son los responsables del envío masivo de correo electrónico no deseado. Ellos obtienen una lista de correos electrónicos a través de bases de datos y empiezan a enviar correo no deseado, que les permite saturar el correo de los usuarios, como también obtener datos del usuario ya que este al darle clic en esos mensajes da permiso para obtener su información personal.

5.3 MARCO LEGAL

Cada día ha venido mejorando la manera de penalizar a los individuos que cometen delitos informáticos en Colombia, debido a que los organismos encargados de implementar las leyes y normativas legales en este país han mirado que este delito se incrementa cada día más.

En Colombia, el tema de la seguridad de la información solo se vino a tratar con rigurosidad hasta el año 2009, con la creación de la Ley 1273 de 2009 “por medio de la cual se modifica el código penal y se crea un nuevo bien jurídico denominado “de la protección de la información y de los datos””[9].

[9] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1-4.

Esta ley fue redactada por el juez segundo de control de garantías Alexander Díaz, experto en nuevas tecnologías del derecho y protección de datos; quien afirma que la ley de delitos informáticos de Colombia es la mejor del continente según el Congreso de la Fiadi (Federación Iberoamericana de Asociaciones de Derecho e Informática).

Con la puesta en marcha de la ley 1273 las empresas y las personas cuentan con un instrumento para poder denunciar, cosa que anteriormente no se hacía, porque los mecanismos existentes no eran los apropiados.

Existen otras normas en la legislación nacional que tratan sobre delitos informáticos y sus penalizaciones, entre ellas están:

- Ley estatutaria 1266 de 2008, "por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales"[10].

- Ley 1341 de 2009, "por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, también con esta ley se crea la Agencia Nacional de Espectro"[11].

[10] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatuaria 1266. (31, diciembre, 2008). Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2008. no. 47219. p. 1-12.

[11] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1341. (30, julio, 2009). Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 2009. no. 47426. p. 1-18.

- Ley 527 de 1999, “por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.”[12]

- Ley estatutaria 1581 de 2012**, “**por la cual se dictan disposiciones generales para la protección de datos personales”[13]. Su implementación y cumplimiento se ejecutan bajo el Decreto 1377 de 2013, en el que se establecen los mecanismos de protección necesarios para la protección de los datos de los usuarios.

[12] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 527. (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial. Bogotá, D.C., 1999.

[13] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatuaria 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D.C., 2012. no. 48587. p. 1-164.

6. METODOLOGÍA DE INVESTIGACIÓN

Para la metodología de investigación de este proyecto de grado, se aplicará una serie de pasos y aspectos que enmarcan cualquier investigación y que sirven para obtener un resultado óptimo y pertinente. Como ya se mencionó anteriormente, el tema de esta investigación es la Ingeniería Social en Colombia.

6.1 TIPO DE INVESTIGACIÓN

Esta es una investigación de tipo analítica y se puede enmarcar, según los criterios de la UNAD, dentro de la línea de investigación de Infraestructura tecnológica y seguridad en redes perteneciente a la Escuela de Ciencias Básicas, Tecnología e Ingeniería. Cuya temática sería la de la Ingeniería Social en Colombia.

A través de esta investigación se pretende realizar un análisis profundo de las diversas técnicas de ingeniería social que año tras año han evolucionado en Colombia y fomentare los buenos hábitos de seguridad, para disminuir los ataques de ingeniería social en las empresas colombianas

Al finalizar esta investigación, se propone entregar un documento con el análisis realizado a la información recolectada acerca de los ataques que han sufrido las empresas colombianas, donde se da a conocer cuáles son las técnicas de ataque más utilizadas en ingeniería social, como identificarlas y como evitarlas a través de los buenos hábitos de seguridad informática.

6.2 METODOLOGIA DE DESARROLLO

La metodología de desarrollo propuesta para esta investigación es por fases, En la fase 1, se debe de recolectar la información acerca de los ataques de ingeniería social en las empresas colombianas, como prioridad seria investigar los más recientes.

En la fase 2, se selecciona la información desde el año más antiguo al más reciente, luego se lee y se analiza la información encontrada.

En la fase 3, se empieza a redactar el documento a entregar a los jurados de evaluación de la tesis, se revisa si se cumplieron los objetivos propuestos en el anteproyecto, por último, se le hace revisión al documento escrito y se hace entrega del informe a los encargados de la evaluación.

7. CRONOGRAMA DE ACTIVIDADES

Tabla 1. Cronograma de actividades para el desarrollo del proyecto titulado Ingeniería Social en las Empresas Colombianas.

CRONOGRAMA DE ACTIVIDADES DEL PROYECTO INGENIERIA SOCIAL EN COLOMBIA				
ACTIVIDAD	**AGOSTO**	**SEPTIEMBRE**	**OCTUBRE**	**NOVIEMBRE**
FASE 1				
Recolectar información acerca de los ataques de ingeniería social en Colombia	**X**	**X**		
FASE 2				
Análisis de la información encontrada		**X**	**X**	
FASE3				
Escritura del proyecto			**X**	**X**
Revisar si se cumplieron los objetivos propuestos				**X**
Entrega del proyecto de grado				**X**

Fuente: Edna Rocio Plazas Garcia.

8. RESULTADOS

8.1 INGENIERIA SOCIAL

Figura. 3 Ingeniería Social.

Fuente: El autor.

8.1.1 Objetivos de la Ingeniería Social

El objetivo general de la aplicación de técnicas de ingeniería social por parte de ciber-delincuentes, es poder ganar acceso no autorizado a las redes o a la información de sus víctimas para lograr su propósito.

Como objetivos específicos de los ataques de ingeniería social llevados a cabo en las empresas colombianas, se tiene:

- Los individuos que aplican las diferentes técnicas de ingeniería social, quieren conseguir beneficios económicos, para poder seguir costeándose las investigaciones y creaciones de malware, ya que para la implementación de virus y de ataques informáticos a gran escala, es necesario invertir una alta suma de dinero si se desea obtener un alto beneficio.

- Otro objetivo es hacer el robo de identidad de una persona, logrando hacker sus redes sociales como Facebook, Instagram, whastapp, etc; para poder tomar el control de su perfil social y poder revisar sus archivos compartidos como fotos, videos, chats.. y luego poder pedirle a la persona afectada alguna remuneración económica, sexuales, o de otra índole, a cambio de no revelar su información privada.

- Así mismo, los delincuentes informáticos realizan ataques de ingeniería social para poder realizar compras en internet, para esto hacen que sus víctimas les den información confidencial de sus tarjetas de crédito (nombres y apellidos, número de cedula, número de tarjeta de crédito, dirección, etc). para ellos poder hacer la transacción y cumplir con su objetivo, conociendo datos importantes de sus víctimas.

- Algunas personas aplican técnicas de ingeniería social para poder obtener el control de una cuenta de correo para enviar correos difamadores, enviar spam, para obtener información que allí se guarde, o simplemente para hacerle el mal a alguien que no le cae bien, etc.

- También buscan acceder gratuitamente a sitios web de Internet que cobran una tarifa para ver videos XXX, jugar, descargar programas, etc. Esto lo logran tan solo con saber el nombre de usuario y contraseña de algún cliente que pague el servicio de internet Banda Ancha.

- Y por último, un objetivo muy perseguido por hackers, es conseguir el control total de un equipo de una empresa para unirlo a una red zombi, para propagar virus, generar spam y cometer otros fraudes en la Red.

8.1.2 ¿Quienes utilizan la Ingeniería Social?

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.

Según el FBI, el acrónimo MICE resume “las distintas motivaciones de los atacantes e intrusos en las redes de ordenadores: Money, Ideology, Compromise y Ego (Dinero, Ideología, Compromiso y Autorrealización personal)”[14].

[14] GÓMEZ VIEITES, Álvaro. Gestión de incidentes de seguridad informática. Madrid: Ra-Ma, 2014. 124 p. ISBN 978-84-9964-331-1.

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.

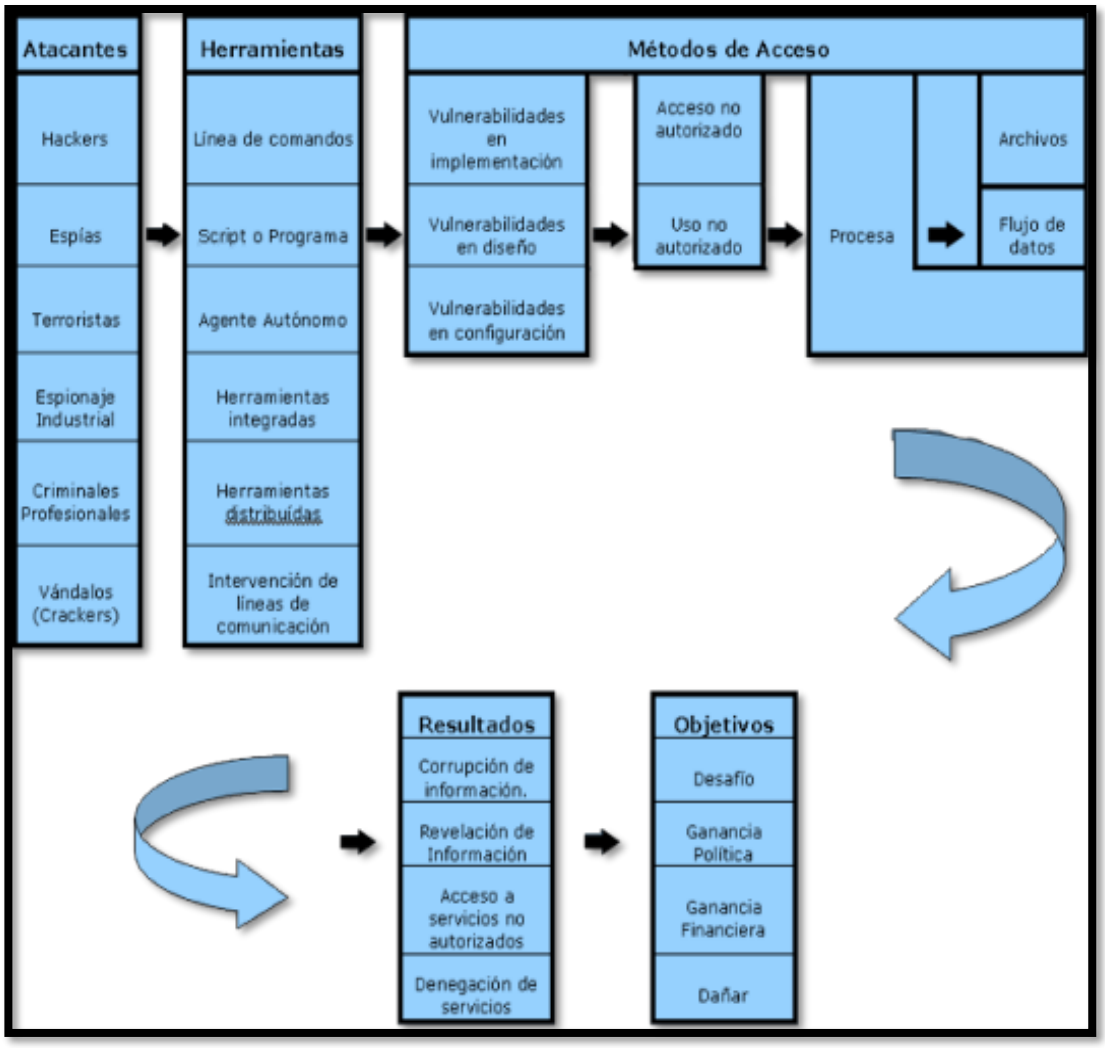
Otros atacantes están convencidos, y persuaden a los demás, de sus doctrinas políticas o religiosas, por las que son capaces de vulnerar sitios gubernamentales o privados. Este caso se vio recientemente en Colombia cuando se descubrió por parte de la Policía Nacional una empresa fachada donde el “hacker”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

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 computaras. Cada uno cuenta con sus propios distintivos y juegan un papel determinado en cada forma de vulnerar la seguridad de la información.

La siguiente imagen exhibe un esquema general de un ataque informático:

Figura. 4 Detalle de un ataque.



Fuente: http://www.segu-info.com.ar/ataques/ataques.htm

8.1.3 ¿Quiénes son los más vulnerables a la Ingeniería Social?

Cualquier empresa, sin importar si es grande o pequeña o si es pública o privada, es vulnerable a sufrir ataques de Ingeniería Social. Si un empleado inconscientemente proporciona información confidencial por medio de un correo

electrónico, de una llamada telefónica o responde a preguntas sospechosas realizadas en una conversación con otra persona, ingenuamente permitirá que el atacante actúe desde el interior o desde el exterior de la empresa, por medio de ataques que rompen las distintas capas de seguridad.

Los ataques de ingeniería social son más seguros en las grandes empresas, pues estas compañías tienen muchos problemas de seguridad informática para manejar sus sistemas de información, ya que poseen infraestructuras de red complejas, ya que estas grandes empresas cuentan con múltiples sucursales, miles de usuarios y diferentes jefes del área TIC (Unos más capacitados que otros). Las políticas de seguridad y los procedimientos a cumplir para el resguardo de la información en estas empresas, son más difíciles de administrar y un atacante puede contactar a distintas personas de esa organización e ir sacando pequeñas cantidades de información a cada empleado.

- Empresas de telefonía
- Hospitales
- Entes gubernamentales
- Instituciones militares
- Entidades financieras
- Empresas de envíos
- Medios de comunicación

Por el contrario, lograr un ataque de Ingeniería social en una empresa pequeña es más difícil, pero no imposible, porque normalmente los empleados se socializan más entre ellos a tal grado que pueden reconocer sus voces en una charla, además de que las políticas de seguridad y los procedimientos se difunden con mayor efectividad a través de los encargados del área de sistemas por medio de

capacitaciones al personal que labora en la compañía (desde las empleadas de aseo generales hasta el gerente).

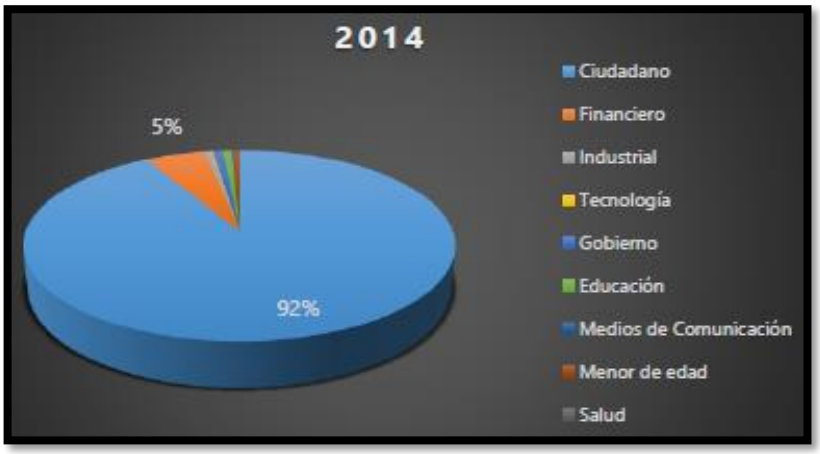
Sin embargo, cualquier persona es vulnerable a ataques de ingeniería social, por medio de sus diferentes técnicas, vía correo electrónico, Internet, por teléfono, SMS, sistemas de mensajería instantánea o simplemente por medio de una charla personal con cualquier "amigo" o cualquier conocido en foros, donde los ciudadanos acostumbran a compartir fotos y datos de lugar y hora de visita a diferentes sitios turísticos; ahí es cuando son marcados como posibles víctimas por los ciber-delincuentes.

8.2 ATAQUES DE INGENIERÍA SOCIAL QUE SE HAN PERPETRADO A LAS EMPRESAS COLOMBIANAS

Durante los últimos 3 años se presentaron 15.565 denuncias por incidentes informáticos en Colombia, según los informes entregados por el Centro Cibernético de la Policía Nacional.

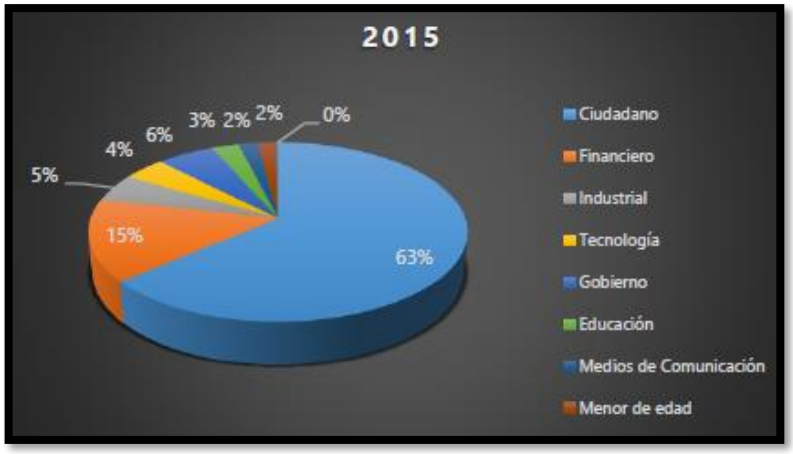
Las víctimas de estos ataques de ingeniería social cambiaron en los últimos años, pasando de afectar al ciudadano de a pie, a afectar a las grandes empresas del sector público y el sector privado, las cuales generan una mayor rentabilidad a la actividad criminal.

Grafica. 1 Porcentaje de denuncias por incidentes informáticos en Colombia en el año 2014



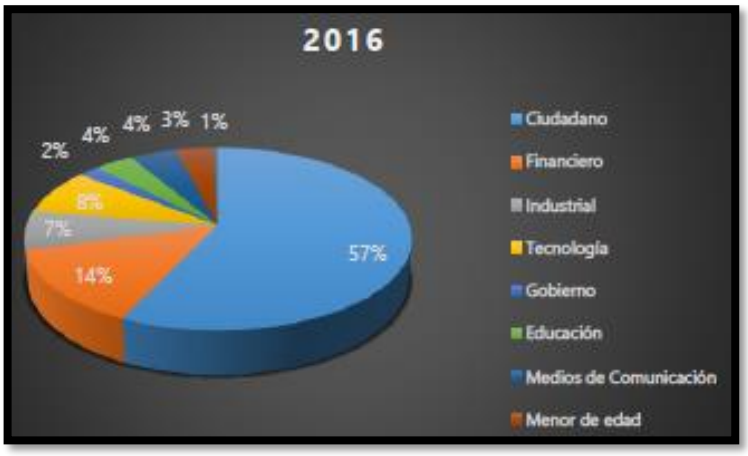
Fuente: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Grafica. 2 Porcentaje de denuncias por incidentes informáticos en Colombia en el año 2015



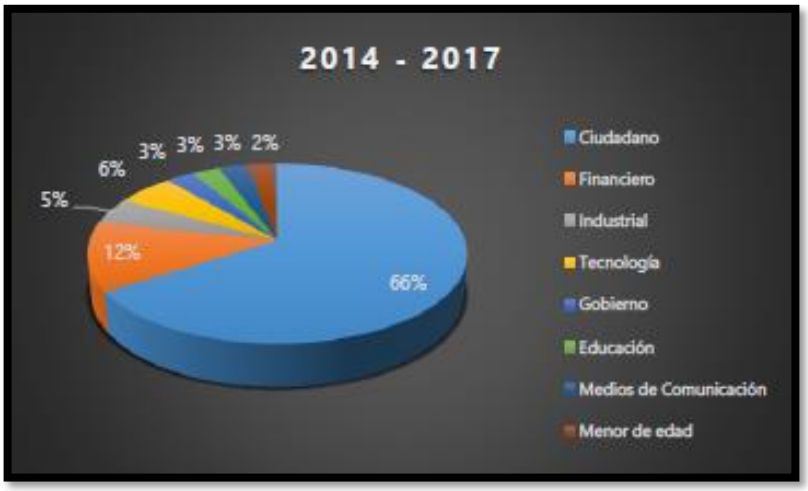
Fuente: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Grafica. 3 Porcentaje de denuncias por incidentes informáticos en Colombia en el año 2016



Fuente: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Grafica. 4 Porcentaje de denuncias por incidentes informáticos en Colombia entre el año 2014 y 2017



Fuente: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

"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 del 35%. Mientras tanto, el sector empresarial pasó de un 5% a un incremento del 28% en los reportes atendidos"[15].

Estas cifras ratifican lo planteado en el documento "*IOCTA 2016*"[16] (Internet Organised Crime Threat Assessment) del European Law Enforcement Agency de EUROPOL, referente a la Tricotomía del delito, en donde se acuerda que a mayor volumen de ataque, con mayor número de víctimas, con nivel de seguridad y protección bajo, el beneficio por ataque es menor.
Pero si el caso es al contrario, donde el ataque se realiza a un sector más pequeño, por ejemplo, el sector financiero, con un ataque más sofisticado, que requiera de mayor habilidad y destreza, con niveles de innovación alto, el beneficio por ataque será mucho mayor.

8.2.1 ¿Cuál es el método de Ingeniería Social que más se está utilizando en Colombia?

"En un año en Colombia, se registran cerca de 198 millones de ataques cibernéticos, es decir, 542.465 ataques diarios"[17].

---

15 POLICIA NACIONAL. Estadística Centro Cibernético Policial. Plataforma de atención a incidentes 24/7 @caivirtual. [En línea] [Citado en 26 de noviembre de 2017.] [En línea]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf.

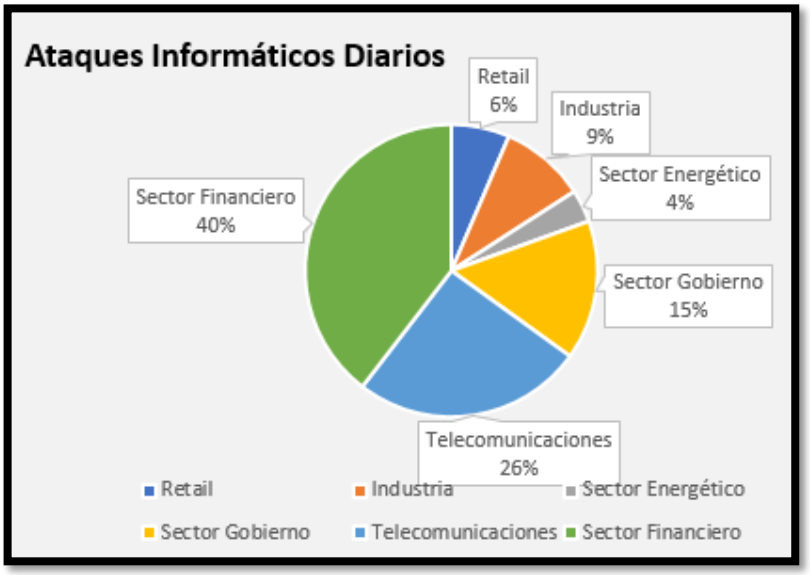
16 EUROPOL. *Internet Organised Crime Threat Assessment OICTA 2016.* [En línea] [Citado el 26 de noviembre de 2017.] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

17 REVISTA DINERO. 2017. Los sectores económicos más impactados por el cibercrimen en Colombia. [En línea] 26 de Septiembre de 2017. [Citado el: 26 de Noviembre de 2017.] http://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321.

Esta estadística pone a Colombia en el tercer puesto de los países más afectados por este tipo de delitos en toda Latinoamérica.

Así se distribuyen los ataques por sectores económicos:

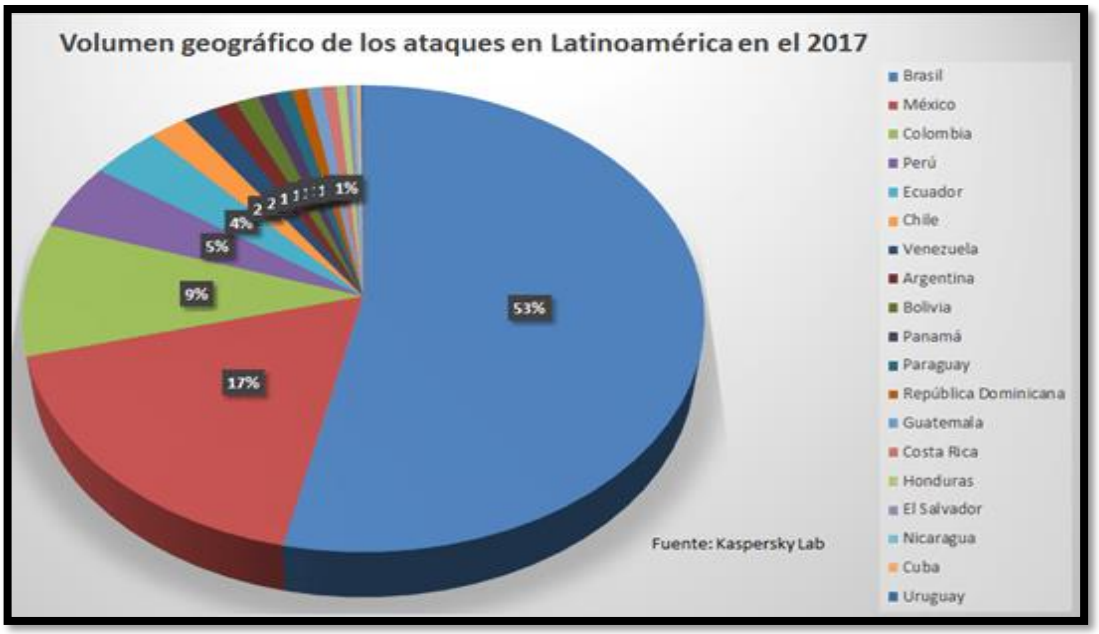
Grafica. 5 Porcentaje de ataques informáticos que ocurren diariamente en Colombia.



Fuente: http://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321

Según un estudio realizado por Karpesky 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.

Grafica. 6 Porcentaje de ataques informáticos en Latinoamérica



Fuente: https://latam.kaspersky.com/blog/33-ataques-por-segundo-kaspersky-lab-registra-un-aumento-de-59-en-ataques-de-malware-en-america-latina/11265/

La técnica más utilizada para robar datos confidenciales de una compañía en Colombia, es la ingeniería social. Según Patricia Gaviria, directora de educación de ETEK International, “esta es una técnica utilizada por varios delincuentes para extraer información confidencial o información sensible de las empresas”[18].

El método de ingeniería social más utilizado por los ciber-delincuentes en Colombia es el 'phising', este método consiste en suplantar cualquier tipo de página web para robar información crediticia o personal por medio de mensajes de correo electrónico que se envían a las víctimas.

[18] GAVIRIA, Paricia. 2017. Pishing, el método de robo por internet más utilizado en el país. *NOTICIAS RCN.* Bogotá : RCN, 11 de Octubre de 2017.

“La cifra de casos de ingeniería social a través del metodo 'phising' aumentó en un 22,6% entre 2015 y 2016, registrando más de 200 denuncias mensuales en la Policía Nacional. La compañía informática RSA señala que este tipo de ataques cibernéticos aumentan entre un 30% y un 40% cada año”[19].

La falta de implementación de programas de concientización en seguridad de la información a directivos y empleados de las diferentes empresas, han convertido al ‘phising’ en una de las causales de ciberdelincuencia más relevantes en 2017; aumentando así los riesgos informáticos en las compañías Colombianas.

8.2.2 Casos de Ingeniería Social ocurridos a empresas Colombianas.

A continuación, se podrá encontrar la descripción de algunos casos de ingeniería social, ocurridos en empresas colombianas en los últimos años.

1. ***Dian (17 de octubre de 2017):*** *E*l 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.

[19] KASPERSKY. 2017. Crecen los Ataques de Phishing en Colombia. [En línea] 22 de Marzo de 2017. [Citado el: 26 de Noviembre de 2017.] http://acis.org.co/portal/content/crecen-los-ataques-de-phishing-en-colombia.

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.

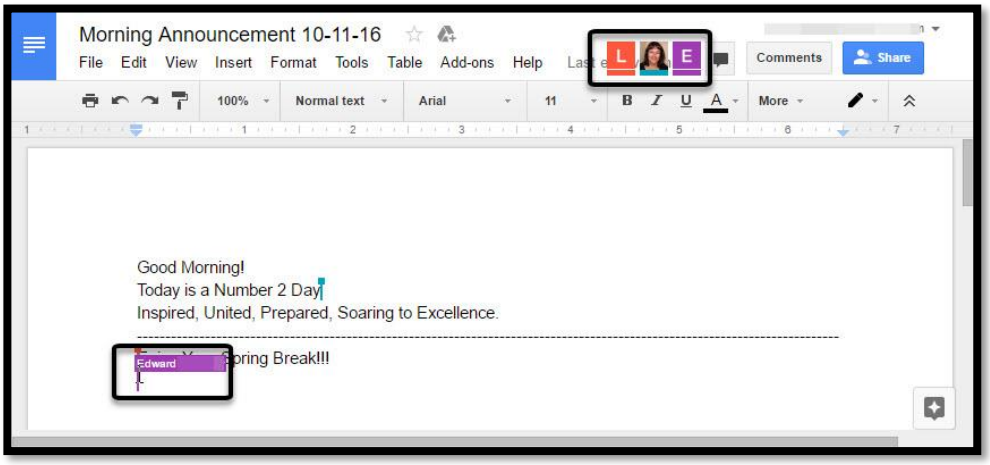
Figura. 5 Mensaje enviado por correo de suplantación de la DIAN

Fuente: El autor.

2. ***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.

Figura. 6 Documento de Google Docs



Fuente:
https://elpais.com/tecnologia/2017/05/04/actualidad/1493887324_006575.html

"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"[20].

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.

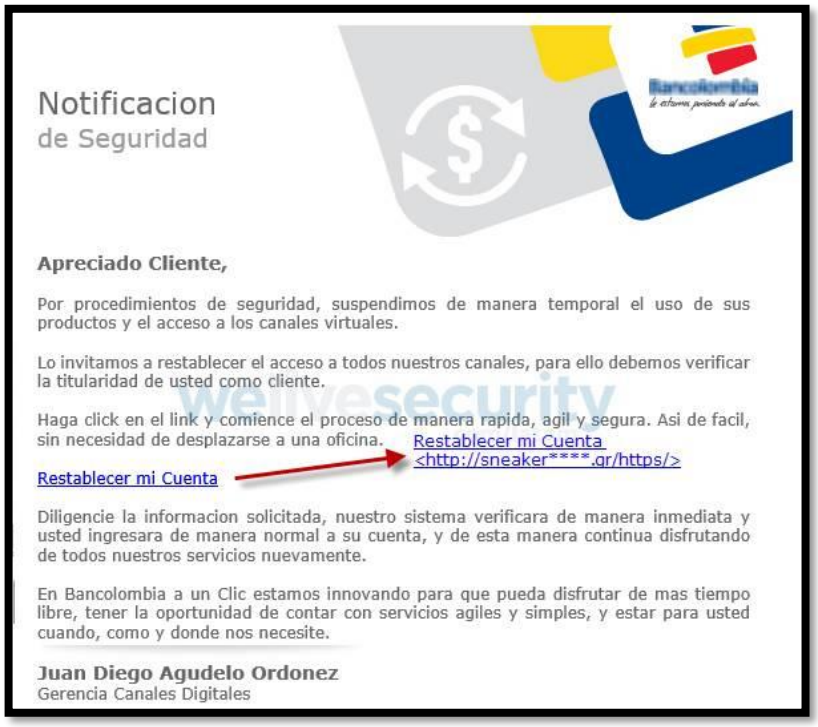
3. ***Bancolombia (13 de marzo de 2017):*** La compañía bancaria Bancolombia sufrió un ataque de pishing el pasado mes de marzo, según investigadores de la firma ESET dicen que este ataque aún se encuentra activo y es una gran amenaza para los más de 10.000.000 de usuarios que cuenta la entidad.

   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

[20] EL PAIS. 2017. *Google Docs sufre un ataque de 'phishing'.* [En línea] 5 de Mayo de 2017. [Citado el: 26 de Noviembre de 2017.] https://elpais.com/tecnologia/2017/05/04/actualidad/1493887324_006575.html.

de bancolombia, logrando ingresar y desviar el dinero que hay en esas cuentas.

Figura. 7 Carta enviada por suplantadores de Bancolombia.



Fuente: http://www.dinero.com/empresas/articulo/campana-de-phishing-afecta-a-miles-de-clientes-de-bancolombia/242871

La figura 3, muestra 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.

4. ***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.

Figura. 8 Ataque informático a la Registraduría Nacional

Fuente: http://www.rcnradio.com/nacional/registraduria-revela-ataque-informatico-origino-fallas-la-pagina-web-la-entidad/

5. ***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.

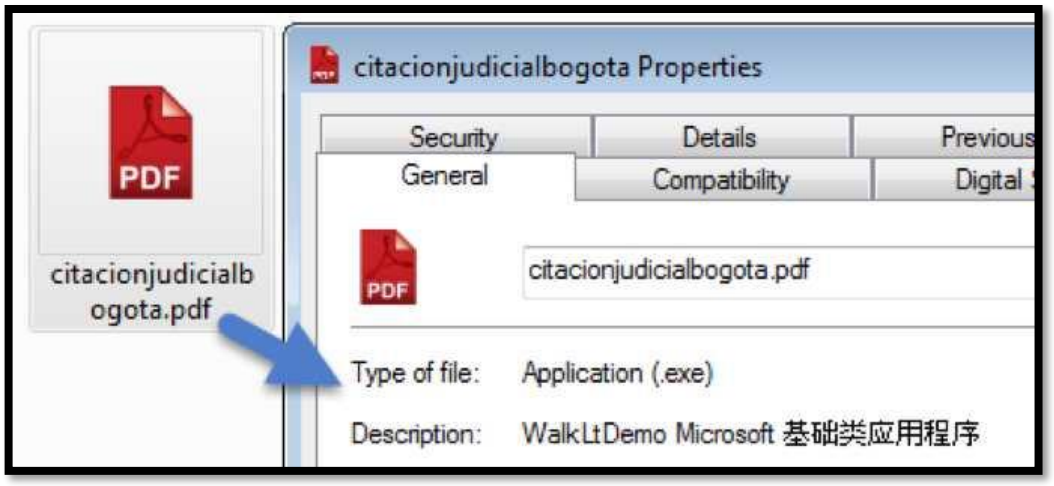
En la supuesta citación hay un mensaje que decía, que por no acudir en los tres llamados que se le hicieron a declarar a la fiscalía, el juzgado le había iniciado un proceso penal en el cual se le judicializaría. Con ese pretexto se le pedía a la víctima que ingresara a través de un enlace que ahí se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

Figura. 9 Citación de la fiscalía utilizada por los ciber-delincuentes.

Fuente: http://www.semana.com/tecnologia/articulo/correos-falsos-de-la-fiscalia/489435

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.

Figura. 10 Archivo de la citación de la fiscalía infectado



Fuente: http://www.semana.com/tecnologia/articulo/correos-falsos-de-la-fiscalia/489435

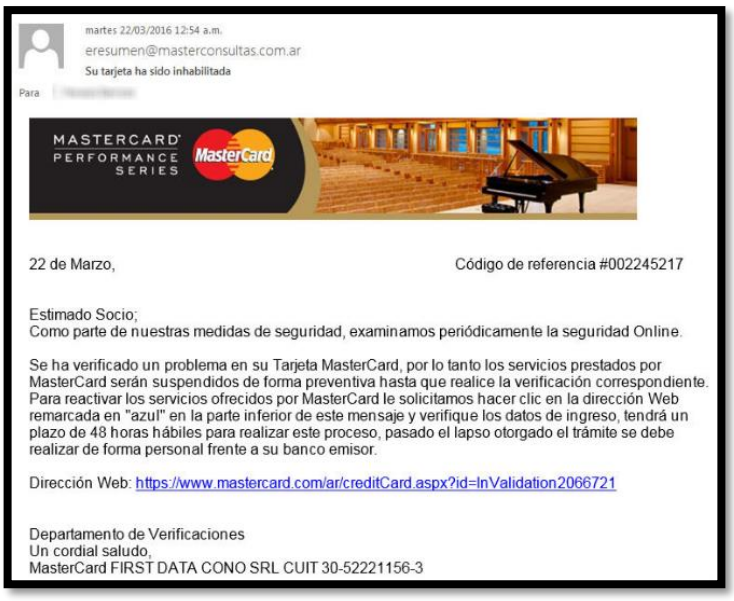
Ante este tipo de hechos, es bueno que las personas sospechen de este tipo de correos, que no los abran de una, qué en vez de dar clic de una buena vez en el enlace, llamen o se acerquen a la entidad y pregunten si de verdad ellos enviaron ese correo. Ya que, si las personas implementáramos hábitos de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

6. ***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 envíar 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 re-direccionado a otro sitio web falso.

Figura. 11 Mensaje enviado por los suplantadores de MasterCard


martes 22/03/2016 12:54 a.m.
eresumen@masterconsultas.com.ar
Su tarjeta ha sido inhabilitada
Para

MASTERCARD PERFORMANCE SERIES

22 de Marzo, Código de referencia #002245217

Estimado Socio;
Como parte de nuestras medidas de seguridad, examinamos periódicamente la seguridad Online.

Se ha verificado un problema en su Tarjeta MasterCard, por lo tanto los servicios prestados por MasterCard serán suspendidos de forma preventiva hasta que realice la verificación correspondiente. Para reactivar los servicios ofrecidos por MasterCard le solicitamos hacer clic en la dirección Web remarcada en "azul" en la parte inferior de este mensaje y verifique los datos de ingreso, tendrá un plazo de 48 horas hábiles para realizar este proceso, pasado el lapso otorgado el trámite se debe realizar de forma personal frente a su banco emisor.

Dirección Web: https://www.mastercard.com/ar/creditCard.aspx?id=InValidation2066721

Departamento de Verificaciones
Un cordial saludo,
MasterCard FIRST DATA CONO SRL CUIT 30-52221156-3

Fuente: http://i64.tinypic.com/wafvgm.jpg

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.

“Eset 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.

8.2.3 ¿Cuál es el tipo de pagó que más piden los delincuentes informáticos a la hora de cobrar sus extorsiones?

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.

[21] EL TIEMPO. 2016. Alerta por correos falsos que atacan a usuarios de MasterCard y Visa. [En línea] 29 de Marzo de 2016. [Citado el: 26 de Noviembre de 2017.] http://www.eltiempo.com/archivo/documento/CMS-16549207.

Figura. 12 Moneda exigida por los ciber-delincuentes "Bitcoins"

Fuente: http://rpp.pe/economia/economia/bitcoin-la-moneda-en-que-piden-rescate-los-hakers-del-ciberataque-mundial-noticia-1050368

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.

"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"[22].

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.

[22] RPP NOTICIAS. 2017. Bitcoin, lamoneda virtual que exigen los hackers tras el ciberataque. [En línea] 12 de Mayo de 2017. [Citado el: 26 de Noviembre de 2017.] http://rpp.pe/economia/economia/bitcoin-la-moneda-en-que-piden-rescate-los-hakers-del-ciberataque-mundial-noticia-1050368.

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”[23].

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 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”[24]. 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.

[23] HERALDO. 2017. ¿Por qué los hackers del ciberataque global exigen los rescates en bitcoins? [En línea] 16 de Mayo de 2017. [Citado el: 26 de Noviembre de 2017.] http://www.heraldo.es/noticias/sociedad/2017/05/16/por-que-bitcoins-1175631-310.html.

[24] RETINA. 2017. Ciberseguridad cinco claves sobre bitcoin y el ataque informatico mundial. [En línea] 14 de Mayo de 2017. [Citado el: 26 de Noviembre de 2017.] https://retina.elpais.com/retina/2017/05/12/tendencias/1494619771_719922.html.

8.3 BUENOS HABITOS DE SEGURIDAD PARA DISMINUIR LOS ATAQUES DE INGENIERÍA SOCIAL EN LAS 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 hacerle 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 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 firewall 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.

9. RECOMENDACIONES

- Se debe de establecer un programa de capacitación referente a la seguridad informática, para todos los trabajadores de las empresas, con el objetivo principal de consolidar una cultura de protección de la información dentro la institución. Estas capacitaciones se deben hacer periódicamente, los encargados de diseñar este programa serán los ingenieros del departamento de TIC y debe estar avalado por los directivos de la compañía.

- Se deben establecer controles de acceso rápido y seguro, como la identificación biométrica, o la identificación electrónica a través de los códigos de barras de los carnets que tienen los empleados de las empresas Colombianas. Si no es posible la instalación de recursos tecnológicos para llevar a cabo la identificación de los empleados a la hora de acceder a las instalaciones de la empresa, se deberá ejercer un control por parte de los guardas de seguridad ubicados en las entradas de las diferentes compañías.

- Es importante tener un gran número de cámaras de seguridad instaladas en los diferentes departamentos de la empresa, para que sean vigilados los archivos confidenciales, los computadores y demás dispositivos que contengan información confidencial de las empresas.

- El reciclaje de los documentos que ya no son útiles en los procesos administrativos de las empresas, deben triturarse, para esto se debe contar por lo menos con una máquina trituradora de papel en la compañía.

Evitando así, que caiga información que pueda ser utilizada por los ingenieros sociales.

- Verificar la correcta actualización de las bases de datos de los antivirus, así mismo se debe revisar el tiempo de caducidad de las respectivas licencias de los antivirus, estas funciones las deben ejercer los encargados del área de sistemas con que cuenta cada compañía Colombiana.

- Buscar la forma de evitar que las redes inalámbricas de las empresas se saturen y se vuelvan focos de inseguridad, que pongan en riesgo tanto a los usuarios como a la información y los activos tecnológicos de las compañías. Para esto se bebe hacer un proyecto que actualice los dispositivos inalámbricos (AP's y "*routers*") y genere redes que cuenten con las medidas de seguridad básica.

- Se deben de administrar de manera centraliza todos los usuarios con privilegios por medio del director de sistemas de la compañía.

- No mantener al alcance de personal no autorizado los puntos de red del cableado estructurado.

- Hacer una política de seguridad donde se restrinja el uso del servicio de internet para los empleados. Esto con el fin de generar grandes beneficios, no solo en lo relacionado con la seguridad, sino también con el rendimiento laboral de todos los empleados de la compañía.

- Implementar un control que evite que los usuarios de la red de la empresa, puedan compartir recursos a través de está.

- Hacer copias de seguridad de manera periódica. Se hace significativo que se concientice a los usuarios para que se limiten a tener en su computador solo la información relacionada con sus actividades diarias empresariales, evitando almacenar información personal que aumentan el tiempo y espacio de las copias de seguridad.

10. CONCLUSIONES

- Al realizar el estudio teórico acerca de los ataques de ingeniería social que se han perpetrado en los últimos años en las empresas colombianas, se logró visibilizar que existen muchas falencias en las empresas colombianas frente al tema de seguridad de la información; ya que estas suelen escatimar en gastos y por eso sufren esos ataques de ingeniería social.

  De la misma manera se logró establecer que el personal de una empresa es el eslabón más débil a la hora de ejecutar un ataque de Ingeniería Social a través de alguna de sus técnicas, ya que a esté se le pueden aplicar técnicas como la suplantación de identidad a través de llamadas telefónicas, de espionaje por encima del hombro, de escuchar detrás de las puertas, entre otras.

- La ingeniería social consiste en obtener información de terceros, sin que estos se den cuenta, es decir, es una manera no convencional de obtener información deseada de manera rápida y segura. Estos ataques suelen ser realizados por grupos de hackers, espías, ciber-delincuentes, detectives privados, etc.

- En este trabajo se describe el análisis realizado para conocer las diferentes técnicas utilizadas a la hora de realizar un ataque de Ingeniería social, quiénes son los más vulnerables a estos ataques, quiénes ejecutan los diferentes métodos de ingeniería social para lograr burlar la seguridad informática de las empresas colombianas. También se describen cuáles son los objetivos de los ingenieros sociales y cuál es el método que más se utiliza en Colombia para el robo de información confidencial.

- Las empresas colombianas que más sufrieron ataques de ingeniería social en los últimos años, son las que pertenecen al sector bancario, ya que estas tienen muchos seguidores por el manejo de recursos económicos que se da en ellas. En la mayoría de los casos ocurridos en las empresas colombianas, los ciber-delincuentes utilizaron el método del PHISHING para el robo de información confidencial, este método consiste en enviar correos electrónicos falsos a cuentas de posibles víctimas, en donde se les solicita a estos que se registren o que accedan a un sitio web suplantado, para luego los ingenieros sociales obtener sus datos de acceso.

- Las empresas Colombianas deben tener un CCTV propio y adicionalmente deben contar con el CCTV de una empresa de vigilancia, ya que no deben quedar puntos ciegos en donde los delincuentes informáticos pueden hacer de las suyas sin quedar evidencia de sus ilícitos. También deben contar con un antivirus licenciado y actualizado, esto no es una garantía total para la protección de la información de una empresa, pero por lo menos reduce el riesgo al que está expuesta. El usuario final debe tomar conciencia y adoptar buenas prácticas a la hora de usar los recursos tecnológicos a su cargo.

- Así mismo se deben implementar políticas de seguridad y medidas de control frente al tema de la seguridad informática y de la información en las empresas Colombianas, a fin de empezar a crear una cultura de protección de la información que permita avanzar, de manera constante, en la evolución y adaptación a los retos que cada día propone el mundo de la tecnología. Por último, se recomienda fomentar los buenos hábitos de seguridad en los empleados de las diferentes empresas colombianas, esto con el fin de disminuir los ataques de ingeniería social en las empresas.

- Los ataques de ingeniería social que se han realizado en los últimos años a las empresas colombianas han ido evolucionando día tras día; ahora los ciber-delincuentes han mejorado la estrategia a la hora de diseñar las imágenes o iframe que van a utilizar en un ataque de phishing, la parte primordial para ellos es diseñar imágenes que sean muy similares a la de la página verdadera esto con el fin de dar confianza a sus víctimas. En un ataque de spoofing, estos delincuentes vienen innovando a la hora de crear los enlaces que les enviaran a sus víctimas a través del correo, ahora utilizan direcciones acortadas y con http para que se parezcan mucho a las páginas que van a suplantar.

REFERENCIAS BIBLIOGRÁFICAS

ARCOS, Sergio. 2011. *Tesís Ingeniería social: Psicología aplicada a la seguridad informática.* Madrid : s.n., 2011.

BANCOLOMBIA. 2017. Ingenieria social. [En línea] 2017. https://www.grupobancolombia.com/wps/portal/personas/aprender-es-facil/seguridad/internet/ingenieria-social/.

BERMUDEZ PENAGOS, Edilberto. 2015. *INGENIERÍA SOCIAL, UN FACTOR DE RIESGO INFORMÁTICO INMINENTE EN.* Neiva : s.n., 2015.

BORGHELLO, Cristian. 2009. “El arma infalible: la Ingeniería Social”. [En línea] Abril de 2009. http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf.

CARUANA, Pablo M. 2017. Breves conceptos sobre la Ingeniería Social. [En línea] abril de 2017. http://www.rompecadenas.com.ar/ingsocial.htm.

CASTELLANOS, Luis. 2009. *Ingenieria social siglo XXI.* 2009.

CONGRESO DE LA REPUBLICA COLOMBIA. 2009. *Ley 1273.* Bogotá : s.n., 2009.

DIGITAL COLOMBIA. 2015. La ingeniería social: el usuario continúa siendo el eslabón más débil. [En línea] 13 de Octubre de 2015. https://colombiadigital.net/actualidad/articulos-informativos/item/8556-la-ingenieria-social-el-usuario-continua-siendo-el-eslabon-mas-debil.html.

DOCPLAYER. Bussines wear en MAC OS X. [En línea] [Citado el: 30 de Septiembre de 2017.] http://docplayer.es/8094891-Businesswear-en-mac-os-x-manual-de-usuario.html.

DRAGONJAR. 2007. Ingenieria social. [En línea] 7 de Octubre de 2007. https://www.dragonjar.org/que-es-ingenieria-social.xhtml.

EDICION NORMAS APA 2016. 2017. normasapa.net. [En línea] abril de 2017. http://normasapa.net/normas-apa-2016/.

EL PAIS. 2017. *Google Docs sufre un ataque de 'phishing'.* [En línea] 5 de Mayo de 2017. [Citado el: 26 de Noviembre de 2017.] https://elpais.com/tecnologia/2017/05/04/actualidad/1493887324_006575.html.

EL TIEMPO. 2016. Alerta por correos falsos que atacan a usuarios de MasterCard y Visa. [En línea] 29 de Marzo de 2016. [Citado el: 26 de Noviembre de 2017.] http://www.eltiempo.com/archivo/documento/CMS-16549207.

—. 2017. Ingeniería social, la razón del éxito de los ladrones digitales. [En línea] abril de 2017. http://www.eltiempo.com/archivo/documento/CMS-16020156.

ENTER. 2016. *Ingenieria social: el hackeo silencioso.* [En línea] 25 de Julio de 2016. http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/.

EUROPOL. *Internet Organised Crime Threat Assessment OICTA 2016.* [En línea] [Citado el: 26 de noviembre de 2017.] https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016.

GAVIRIA, Paricia. 2017. Pishing, el método de robo por internet más utilizado en el país. *NOTICIAS RCN.* Bogotá : RCN, 11 de Octubre de 2017.

GONZALEZ JUAREZ & PEÑA ENRIQUEZ, Diego Dante & José Antonio. 2012. *ESTUDIO DEL IMPACTO DE LA INGENIERÍA SOCIAL - PHISHING.* Mexico : s.n., 2012.

HERALDO. 2017. ¿Por qué los hackers del ciberataque global exigen los rescates en bitcoins? [En línea] 16 de Mayo de 2017. [Citado el: 26 de Noviembre de 2017.]

http://www.heraldo.es/noticias/sociedad/2017/05/16/por-que-bitcoins-1175631-310.html.

IDEASGEEK. 2017. Top de las técnicas de ingenieria social usadas por los scammers. [En línea] abril de 2017. http://www.ideasgeek.net/2009/11/16/top-de-las-tecnicas-de-ingenieria-social-usadas-por-los-scammers/.

KASPERSKY. 2017. Crecen los Ataques de Phishing en Colombia. [En línea] 22 de Marzo de 2017. [Citado el: 26 de Noviembre de 2017.] http://acis.org.co/portal/content/crecen-los-ataques-de-phishing-en-colombia.

LA REPUBLICA. 2015. Ingeniería social. [En línea] 4 de septiembre de 2015. http://www.larepublica.co/ingenier%C3%ADa-social_240786.

LAUINGER, Tobias. PANKAKOSKI, Veikko. BALZAROTTI, Davide. KIRDA, Engin. 2010. *Honeybot, Your Man in the Middle for Automated Social Engineering.* Francia : s.n., 2010.

LONDOÑO, Cesar Jaramillo. 2017. *La ingenieria social: Un desafío investigativo.* Bogota : s.n., 2017.

MINTIC. 2016. Mintic. *Ingenieria social.* [En línea] 30 de Septiembre de 2016. http://www.mintic.gov.co/portal/604/w3-article-18800.html.

NOHLBERG, Marcus. 2088. *Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks.* Estocolmo : s.n., 2088.

OPENBSDCOLOMBIA. 2010. Ingenieria social. [En línea] Diciembre de 2010. http://www.openbsdcolombia.org/documentos/others/IngenieriaSocial_CasodeEstudio.pdf.

PEARSON, Dale. 2010. Social Engineering, Mentalism, Hypnosis, Misdirection and Influence. [En línea] 2010. http://www.subliminalhacking.net/.

PENAGOS BERMUDEZ, Edilberto. 2015. *INGENIERÍA SOCIAL, UN FACTOR DE RIESGO INFORMÁTICO INMINENTE EN.* Neiva : Tesis de grado Especializacion, 2015.

POLICIA NACIONAL. Estadística Centro Cibernético Policial. Plataforma de atención a incidentes 24/7 @caivirtual. [En línea] [Citado el: 26 de noviembre de 2017.] https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf.

RETINA. 2017. Ciberseguridad cinco claves sobre bitcoin y el ataque informatico mundial. [En línea] 14 de Mayo de 2017. [Citado el: 26 de Noviembre de 2017.] https://retina.elpais.com/retina/2017/05/12/tendencias/1494619771_719922.html.

REVISTA DINERO. 2017. Los sectores económicos más impactados por el cibercrimen en Colombia. [En línea] 26 de Septiembre de 2017. [Citado el: 26 de Noviembre de 2017.] http://www.dinero.com/empresas/articulo/sectores-mas-afectados-por-cibercrimen-en-colombia/250321.

REVISTA EMPRESARIAL & LABORAL. 2017. Riesgos Emergentes: ataques de ingeniería social en cuentas bancarias. [En línea] abril de 2017. https://revistaempresarial.com/tics/redes-sociales/riesgos-emergentes-ataques-ingenieria-social-cuentas-bancarias/.

REVISTA SEMANA. 2017. Conozca de qué se trata la 'ingeniería social' y tome precauciones. [En línea] abril de 2017. http://www.semana.com/tecnologia/tips/articulo/conozca-que-trata-ingenieria-social-tome-precauciones/373280-3.

RPP NOTICIAS. 2017. Bitcoin, lamoneda virtual que exigen los hackers tras el ciberataque. [En línea] 12 de Mayo de 2017. [Citado el: 26 de Noviembre de 2017.] http://rpp.pe/economia/economia/bitcoin-la-moneda-en-que-piden-rescate-los-hakers-del-ciberataque-mundial-noticia-1050368.

SANTAMARIA, Ernesto Emiliano. 2008. Ingenieria social. [En línea] 20 de Septiembre de 2008. http://procedimientospolicialescolombia.blogspot.com.co/2008/09/ingenieria-social.html.

SCRIBD. 2017. La Ingeniería Social “Oportunidades que le brindan las nuevas amenazas". [En línea] abril de 2017. http://www.scribd.com/doc/16235960/Ingenieria-Social-Oportunidades-que-le-brindan-las-nuevas-amenazas.

SIC. 2017. Seguridad de la Informacion en Colombia. [En línea] abril de 2017. http://seguridadinformacioncolombia.blogspot.com/2010/06/fundamentos-de-ingenieria-social.html.

SIMON, Kevin . MITNICK William L. 2005. *The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers.* USA : s.n., 2005.

TEAM CYMRU RESEARCH NFP. 2011. Malicious Activity Maps. [En línea] 2011. http://www.team-cymru.org/Monitoring/Malevolence/maps.html.

UNIVERSIDAD NACIONAL DE COLOMBIA. 2011. Ingeniería social y sostenible para Colombia. [En línea] 8 de Julio de 2011. http://agenciadenoticias.unal.edu.co/detalle/article/ingenieria-social-y-sostenible-para-colombia.html.

VALDIVIA, Martin. 2014. Ingenieria social aplicada al delito informatico. 2014.

VISENTINI, Maximiliano. 2006. *La ingenieria social "Oportunidades que le brindan las nuevas amenazas".* Cordoba : s.n., 2006.

WEBSECURITY. 2017. La Ingeniería social (Introducción). [En línea] abril de 2017. http://www.websecurity.es/ingenier-social-introducci-n.

WIKIPEDIA. 2017. Ingeniería social (seguridad informática). [En línea] abril de 2017. https://es.wikipedia.org/wiki/Ingenier%C3%ADa_social_(seguridad_inform%C3%A1tica).