DELITOS INFORMÁTICOS ASOCIADOS A LA INGENIERÍA SOCIAL EN COLOMBIA Y LATINOAMÉRICA

MARTHA YANETH IBARRA IMBACHI

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA D.C.
2018

DELITOS INFORMÁTICOS ASOCIADOS A LA INGENIERÍA SOCIAL EN COLOMBIA Y LATINOAMÉRICA

MARTHA YANETH IBARRA IMBACHI

Monografía como proyecto de Grado para optar al título de
Especialista en Seguridad Informática

Directora
HELENA CLARA ISABEL ALEMÁN NOVOA
Ingeniera de Sistemas

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
BOGOTA D.C.
2018

Nota de Aceptación:

_____

_____

_____

_____

_____

_____

Firma del presidente del Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Bogotá, D.C. 31 de octubre de 2018

CONTENIDO

pág.

INTRODUCCIÓN

La ingeniería social puede ser definida como todas las técnicas, suplantaciones y metodologías que son utilizadas para engañar y lograr identificar puntos vulnerables de la seguridad, con esto, se tiene acceso a contraseñas, usuarios e información confidencial que es utilizada contra el vulnerado bien sea directa o indirectamente.

Este conjunto de actividades o engaños que realizan los atacantes a las organizaciones y/o personas se usan para obtener información personal o de los bienes de las entidades utilizando las credenciales autorizadas para acceder a la información. Entiendo que la Ingeniería Social es la ciencia o el arte de hackear a las personas.

A pesar de que la tecnología avanza de manera significativa y con ella las herramientas que mitigan las diferentes vulnerabilidades informáticas, muchas veces nos olvidamos de un recurso vital en toda la industria que es la del ser humano. Por lo tanto, es importante que las personas tomen conciencia del peligro que circula en nuestro entorno y que es responsabilidad de cada usuario tomar las medidas y precauciones necesarias para prevenir estos ataques.

El éxito que se tiene en los engaños realizados se logra obteniendo la mayor parte de información confidencial y personal de alguien la cual es utilizada creando situaciones supuestas sin que las mismas sean reales y de esta manera se hace la suplantación de una persona e inclusive de empresas.

La mayor parte de fraudes realizados con esta metodología es realizada vía telefónica, a través de falsos funcionarios de entidades o utilizando mensajes de texto con teléfonos celulares.

La Ingeniería Social es tan eficiente y efectiva que ocupa un porcentaje importante en la mayoría de los ciberataques dirigidos a la población Colombiana

y Latinoamericana. Siendo la información uno de los activos más importantes de las entidades, es uno de los principales objetivos de ataques de los delincuentes, evidenciado pérdidas significativas de miles de millones de pesos con estos ataques.

Los problemas y ataques de seguridad se están incrementando de una manera rápida y prominente, porque a pesar que hay conocimiento del tema, se piensa que nunca les va a pasar y la autoformación o formación por parte de las entidades no tiene el peso que debería tener.

Dentro del presente documento se pretende hacer un reconocimiento de los tipos de delitos informáticos aplicados mediante la ingeniería social, hacer un estudio de las técnicas mayormente utilizadas en dichos delitos, al igual que los aspectos que hacen que una persona sea víctima de estos ataques, todo esto conllevará a la realización de un análisis de esta problemática en donde se identifiquen las leyes colombianas que castigan este tipo de comportamientos y la mejor manera de prevenirlos.

1. TITULO DEL PROYECTO

DELITOS INFORMÁTICOS ASOCIADOS A LA INGENIERÍA SOCIAL EN COLOMBIA Y LATINOAMÉRICA. DEFINICIÓN DEL PROBLEMA

2. DEFINICIÓN DEL PROBLEMA

2.1 ANTECEDENTES DEL PROBLEMA

Cuando se hace referencia al termino ingeniería social se ha podido referir a dos tipos de vías, la primera que va en la forma de implementar programas de implementaciones social y la segunda en los diferentes esfuerzos que contribuyen en la influencia de actitudes, relaciones o acciones sociales que se pueden dar en una comunidad, región o país, estos dos sentidos han sido bastante usados en materia de ciencias políticas.

El termino ingeniería social presenta en la actualidad una connotación negativa teniendo en cuenta que se asocia con comportamientos ilegales o contradictorios a las normas establecidas, pero es necesario precisar que a pesar de esto, se pueden tener organizaciones o individuos que buscan cambiar y aplicar diferentes puntos para mejora de la sociedad en la que se encuentra, por ejemplo se tienen los casos de la competencia en algún negocio en donde la contrapartida puede implementar temas de ingeniería social para perjudicar o no a su contrincante, estos mismos casos se dan en la vida cotidiana o en las organizaciones.

Según el artículo “Ingeniería social – El hackeo al ser humano. Un enfoque holístico”[1] el origen de esta expresión se da en 1894, por un filántropo y empresario de nombre holandés J.C. Van Marken, continúo siendo esparcido en el país de Francia por alguien llamado Émile Cheysson y su mayor apropiación se dio cuando el reformista social W.H. Tolman lanzo su libro de nombre “*Social Engineering*”. Los primeros inicios del concepto tuvieron base en que las

[1] LEDESMA, Cristina. “Ingeniería social – El hackeo al ser humano. Un enfoque holístico”. {En línea}. {10 de octubre de 2014}. Disponible en (http://www.magazcitum.com.mx/?p=2747#.WvZWHqTt7IU)

empresas de la época no tenían grandes interacciones con las obras sociales, es por eso por lo que Tolman tuvo la tarea de servir de mediador realizando una labor social entre las dos partes.

A partir del siglo XIX, poniendo en práctica los conceptos de diferentes pensadores liberales, el termino y concepto se generaliza a que refiere a métodos que buscan obtener una variedad de resultados, lo que quiere decir que ya no se ve solo como instrumento para resolver problemas sociales y se convierte en el uso de técnicas que buscan manipular a las personas en su vida cotidiana.

2.2 FORMULACIÓN DEL PROBLEMA

En Colombia y en Latinoamérica, actualmente se tiene una amenaza bastante grande relacionada con los delitos de los que la ciudadanía está siendo víctima sin darse cuenta. Muchas veces de manera indirecta se brinda información confidencial que termina siendo aprovechada por delincuentes para asaltar, robar, secuestrar información en busca de su propio beneficio.

En primer lugar, es clave entender que en el momento en que cuando se habla de ingeniería social, se referencia a todo un conjunto de diferentes habilidades y técnicas psicológicas de las personas que son usadas conscientemente para obtener información personal de las demás personas de manera ilegal.

La población colombiana en la actualidad está siendo víctima de personas malintencionadas que hacen uso de la ingeniera social usando técnicas, suplantaciones y metodologías que son utilizadas para engañar y lograr identificar puntos vulnerables de la seguridad, con esto, se tiene acceso a contraseñas, usuarios e información confidencial que es utilizada contra el vulnerado bien sea directa o indirectamente.

El éxito que se tiene en los engaños realizados se logra obteniendo la mayor parte de información confidencial y personal de alguien quien es utilizado creando situaciones supuestas sin que las mismas sean reales y de esta manera se hace la suplantación de una persona e inclusive de empresas. La mayor parte de fraudes realizados con esta metodología es realizada vía telefónica, a través de falsos funcionarios de entidades o utilizando mensajes de texto con teléfonos celulares.

Esta es una problemática que las personas no han logrado controlar y que cada día crece afectando más duramente la seguridad e integridad de la población. Es por eso por lo que a través de este documento se podrá llevar una idea de:

¿Cuáles son los aspectos más críticos de la ingeniería social, sus técnicas y cuáles son las mejores maneras de afrontarlas?

Es importante dar a conocer las metodologías que evitan ser víctimas de ataques informáticos aplicados a través de la ingeniería social, puesto que estos son medios que contribuyen en la vida personal, familiar y laboral de cualquier persona. La realidad actual, exige en las personas acciones concretas para no seguir siendo usuarios sin conciencia, si no por el contrario concientizar a las personas de la importancia de cuidar la información como activo para el crecimiento de las empresas y la vida personal.

2.3 DESCRIPCIÓN DEL PROBLEMA

Teniendo en cuenta que cuando se habla de ingeniería social, se refiere a las diferentes técnicas psicológicas usadas para conseguir información personal y confidencial de las demás personas haciendo uso de sus habilidades[2], se ha podido identificar que actualmente, la población en Colombia y en Latinoamérica está siendo víctima de personas malintencionadas que hacen uso de la ingeniera social por medio de técnicas, suplantaciones y metodologías que son utilizadas para engañar y lograr identificar puntos vulnerables de la seguridad, con esto, se tiene acceso a contraseñas, usuarios e información confidencial que es utilizada contra el vulnerado bien sea directa o indirectamente[3]. El éxito que se tiene en los engaños realizados se logra obteniendo la mayor parte de información confidencial y personal de alguien quien es utilizado creando situaciones supuestas sin que las mismas sean reales y de esta manera se hace la suplantación de una persona e inclusive de empresas. La mayor parte de fraudes realizados con esta metodología es realizada vía telefónica, a través de falsos funcionarios de entidades o utilizando mensajes de texto con teléfonos celulares.

Esta es una problemática que las personas no han logrado controlar y que cada día crece afectando más duramente la seguridad e integridad de la población.

[2] HACK, Story. “Ingeniería Social”. {En línea}. {22 de julio de 2013}. Disponible en (https://hackstory.net/Ingenier%C3%ADa_social)
[3] ROMERO, Op. cit. Disponible en: (http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/)

3. JUSTIFICACIÓN

La ingeniería social es un problema social que ha resultado bastante complejo a los latinoamericanos y en concreto los colombianos se han tenido que enfrentar y han venido siendo el resultado del manejo no adecuado de la comunicación y las tecnologías de la información, esto teniendo en cuenta que las personas no tienen la conciencia de protegerse y de la misma manera proteger su información personal.

Esto tiene que ver con la falta de conocimiento, la falta de información y el mal manejo de la información confidencial que son puntos clave para evitar ser víctimas de delitos informáticos más específicamente de delitos aplicados mediante ingeniería social. Por esta razón, es necesario que se brinden soluciones para que se contrarresten y se prevengan este tipo de ataques.

El uso de la ingeniería social es uno de los ataques más utilizados teniendo en cuenta que se manipula directamente a una persona y no a un sistema. Un sistema puede estar protegido con los mejores antivirus y los mejores software antimalware, así como firewalls y cualquier otro sistema, tecnología o software que proteja los equipos, pero ninguna de estas alternativas puede resistir a un buen ataque de ingeniería social, dado que no va directamente al ordenador en sí, sino hacia la persona que lo controla. La ingeniería social busca influenciar a una persona para que resulte haciendo o diciendo cosas estrictamente confidenciales que afectan a la persona que es víctima del ataque.[4]

Este, es uno de los ataques más conocidos y más explotados; se trata de manipular a personas, persuadiéndolas o influenciándolas para que hagan cosas que no deberían hacer. Todo esto se consigue generando una situación creíble,

[4] OSEANO-It. “La importancia de protegerse contra los ataques de ingeniería social”. {En línea}, {2014}. Disponible en: (http://www.oceano-it.es/news-individual/371/protegerse-contra-ataques-de-ingenieria-social)

donde todo está estudiado hasta el más mínimo detalle. [5]Día a día la tecnología presenta a la población colombiana grandes avances que van en crecimiento y a su vez brindan muchas facilidades para realizar tareas de la vida diaria como lo es por ejemplo la realización de compras online a través de apps que ofrecen comodidad a los usuarios. Estas son soluciones tecnológicas que a su vez dan más oportunidad de que existan y se generen ataques informáticos a redes vulnerables y con fácil acceso robando así información confidencial de las personas y que deben estar acompañadas de las prevenciones necesarias para evitar ser víctima de cualquier actividad fraudulenta.

Por estas razones, se genera la necesidad de brindar herramientas básicas para la población colombiana y latinoamericana con las cuales logren contrarrestar los intentos de fraude que se quieran generar. A su vez, se debe conocer que es importante tener cuidado con la información personal, y que a su vez es fundamental dar a conocer técnicas para evitar ser víctima de ingeniería social, reconociendo a este como una de las técnicas más efectivas para cometer fraudes en el mundo.

Teniendo en cuenta que la manera correcta de tratar los datos, la seguridad de estos y el correcto funcionamiento del servicio son los principales objetivos de la seguridad informática, se ha podido identificar que es necesario realizar intervenciones que contrarresten los malos usos de ingenieros sociales quienes son los encargados de realizar intervenciones y sustraer información lo cual lo logran a través de la implementación de diferentes estrategias propias de su entrenamiento. Esto [6]hace que la seguridad informática sea parte fundamental para contrarrestar estas técnicas y avanzar hacia un país mucho más seguro.

[5] Oceano It, Disponible en: (http://www.oceano-it.es/news-individual/371/protegerse-contra-ataques-de-ingenieria-social)
[6] HACK Story. Op. cit. Disponible en: (https://hackstory.net/Ingenier%C3%ADa_social)

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Realizar el estudio analítico de delitos informáticos asociados con técnicas de ataques aplicados a través de ingeniería social en Colombia y Latinoamérica.

4.2 OBJETIVOS ESPECÍFICOS

1. Identificar los tipos de delitos informáticos aplicados mediante la ingeniería social aplicados en Colombia y Latinoamérica.

2. Reconocer las leyes que rigen en Colombia y Latinoamérica los delitos informáticos enmarcados en la ingeniería social.

3. Analizar las técnicas utilizadas para la realización de delitos de ingeniería social concientizando a las personas de los riesgos a los que se exponen día a día.

4. Identificar cuáles son los aspectos más relevantes que hacen que una persona sea víctima de delitos de ingeniería social evitando el fraude informático en la población en general.

5. MARCO REFERENCIAL

5.1 ESTADO ACTUAL

En Latinoamérica, se ha vuelto bastante común la realización de transacciones electrónicas online teniendo en cuenta el gran avance que está teniendo la tecnología y las redes. Muchas personas son conscientes de la necesidad de contar con seguridad y las mejores prácticas para fomentarla, sin embargo, muchas de estas aun no tienen dicha conciencia o dicho conocimiento. Es importante conocer que las empresas y organizaciones están uniendo esfuerzos para el mejoramiento continuo y la generación de esquemas que contribuyan con la prevención que eviten ser víctimas de dichos delitos.

Los ataques realizados a través de la ingeniería social y sus diferentes técnicas pueden clasificarse en ataques pasivos, ataques activos o riesgos.

Los primeros se basan en la afectación a la confidencialidad de la información teniendo en cuenta que en este tipo de ataques consisten en observar la información sin tener acceso a ella ni realizar algún tipo de alteración a la misma.[7]

Los segundos, están basados en la afectación al principio de integridad de la información al igual que su autenticidad, esto teniendo en cuenta que no solo se realiza una labor de observación si no por el contrario se realizan modificaciones y alteraciones a la misma. Por último, se tienen los riesgos los cuales son reconocidos por contar con la posibilidad de que una amenaza se realice o no, esto se da aprovechando las vulnerabilidades que el sistema o la información presenten.

[7] SORIANO, Miguel. “Seguridad en redes y seguridad de la información”. {En línea}. {2017}. Disponible en: (http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf.)

5.2 MARCO TEORICO

5.2.1 Concepto de ingeniería social. El término ingeniería social puede sustraerse de dos formas que se han podido identificar con el paso del tiempo, en primer lugar, se refiere a la informática como tal o puede leerse en el término especifico de los hackers y la segunda puede sustraerse del ámbito de las ciencias políticas.

En el primer caso, se pueden identificar hackers que en resumen se pueden clasificar como “buenos o malos”, estos tienen que ver con las personas que se dedican a la seguridad informática en su totalidad, pero específicamente a las distintas maneras de violentarla haciendo uso de técnicas psicológicas y tecnológicas para obtener información no autoriza. En el segundo caso, se ha visto la intervención de las ciencias políticas tiene que ver con el modo de infundir acciones, actitudes y modos de actuar o pensar en la sociedad para lograr que esta piense de una manera específica.[8]

En la actualidad, la ingeniería social es reconocida como la práctica de manipular a las personas para realizar suplantaciones, engaños y de esta manera obtener información confidencial, dejando al descubierto puntos de mayor vulnerabilidad en la seguridad. Con esto, se tiene acceso a contraseñas, usuarios e información confidencial que es utilizada contra la víctima bien sea directa o indirectamente.

La mayor parte de estos ataques son realizados a través de correo electrónico o haciendo uso de llamadas telefónicas. El éxito que se tiene en los engaños realizados se logra obteniendo la mayor parte de información confidencial y personal de alguien, esta a su vez se usa creando situaciones supuestas y/o ficticias y de esta manera se hace la suplantación de una persona e inclusive de empresas con alto estándares de seguridad implementados.

[8] OJEDA, Cesar. “Psicología y Mente. Ingeniería social: ¿el lado oscuro de la Psicología?” {En línea}, {02 de noviembre de 2017}. Disponible en: (https://psicologiaymente.net/social/ingenieria-social-psicologia)

La ingeniería social puede ser usada contra individuos y de la misma manera contra empresas sin importar si estas son grandes o pequeñas. Un atacante busca un personaje para imitar, arma un libreto que sea convincente y como estos ataques son mucho más humanos, las herramientas tecnológicas no son suficientes para su prevención.

5.2.2 Principios de la ingeniería social[9]. La manifestación de las personas en la cual se tiene la premisa de querer brindar alguna ayuda.

La confianza que se debe crear con la victima a la cual se va a realizar el ataque, esto es fundamental para la continuidad de la situación que se planea.

La premisa que se tiene de las personas al no saber contestar con un NO a una situación extraña o ajena.

Tiene que ver con la situación donde el atacante alaga a la víctima y está a su vez se siente con demasiado ego y accede a alguna petición.

5.2.3 Procesos dentro de contexto de ingeniería social[10]. Dentro del proceso de ingeniería social se pueden tener contextos como:

Noticias falsas, o fake news.
Permite redirigir consultas o información con falsas noticias o promesas de haberte ganado algo, por ejemplo, clickea aquí has ganado un viaje a San Andrés.

[9] DELGADO, Javier. “Los 4 principios básicos de la Ingeniería Social”. {En línea}, {27 de agosto de 2008}. Disponible en: (http://unpocodemucho.com/los-cuatro-principios-basicos-de-la-ingenieria-social)
[10] MEDINA, Edgar. “Ingeniería social, la razón del éxito de los ladrones digitales”. {En línea}, {29 de junio de 2015}. Disponible en: (http://www.eltiempo.com/archivo/documento/CMS-16020156)

5.2.3.1 El proceso de phishing por medio de correos electrónicos. Muchas veces se ofrecen premios debido a que de alguna forma tienen la información y saben que productos se tiene, con esos bancos explotan esa información por medio de cuentas de correo falsas y redirigiendo información a un portal similar al del banco de uso de la víctima.

5.2.3.2 Llamadas telefónicas. Busca hacer acreedores a las personas de un premio o una situación familiar exigiendo dinero a cambio del premio o informando acerca de algún peligro que corre un familiar.

5.2.3.3 Consultas dentro de las redes sociales. Muchas veces la gente publica información que puede ser sensible y puede ser tomada para realizar procesos de ingeniería social, por ejemplo, el publicar una foto en un sitio en específico, el atacante usara esta información para identificar tu sitio y así realizar el proceso de ataque como una llamada telefónica extorsionando o el posible secuestro de un familiar.

5.2.3.4 Sexualidad. Muchos atacantes usan videos de mujer voluptuosas y comienzan el ataque por medio de chats o servicios de mensajería como WhatsApp o Skype, simulan realizar chats de video y graban todo para luego pedirles sumas de dinero con el fin de no compartir esa información con sus familiares amigos o incluso en trabajos.

Existen dos modos de realizar ingeniería social, el primero está enfocado al acceso y extracción de información de un computador sin tener ningún de autorización y la segunda relacionándose directamente con las personas y obteniendo datos de confiabilidad haciendo uso de engaños. [11] Teniendo en cuenta esto, se pone en práctica diferentes fases que van desde ganar la confianza de la víctima, estar en un estado de alerta para poner conocer la manera de actuar de la víctima y por último una distracción en la cual se distraiga

[11] PISCITELLI, Emiliano. “Edición 293 de revista USERS”. {En línea}, {04 de diciembre de 2015}. Disponible en: (http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/)

a la víctima para que pierda conexión con la alerta generada. Por otra parte, la aplicación de la ingeniería social en computadoras se implementa usando diferentes técnicas de fraude que se pueden dar desde diferentes usuarios en dominios, email, páginas web, etc.

Se ha sabido hoy en día que grandes hackers aseguran que no tiene ningún sentido ni justificación invertir dinero en tratar de romper la seguridad de los sistemas informáticos sean robustos o no, por el contrario, resulta mucho más rentable ejecutar ataques de ingeniería social para obtener credenciales de acceso y de esta manera romper los estándares de seguridad implementados sin violentarlos.

5.3 MARCO CONCEPTUAL

Para contextualizar, la ingeniería social relaciona la práctica de acceder información o datos confidenciales por medio del uso de estrategas que resultan en la manipulación de los usuarios o de cualquier persona. Se puede decir que uno de los principales fines y para los que más se hace uso de esta metodología es para el hurto de dinero o elementos de valor, esto, no limita que pueda ser usado por diferentes medios como lo son páginas de internet, portales web, cajeros automáticos, bancos, entidades financieras, etc. En este orden de ideas, esto se cataloga como delitos de robo de identidad a pesar de que no en todos los países de américa latina se cuenta con legislación específica para catalogar como delitos este tipo de comportamientos.

Se puede evidenciar el crecimiento desbordado del mal uso de la ingeniería social, pues se reconoce también como el arte de hackear a seres humanos lo cual está siendo muy fácil teniendo en cuenta el mal uso que se da a las redes sociales, correos electrónicos u otros medios de comunicación por los que se puede hurtar información.[12]

[12] Ingeniería social. “Ingeniería social, hackeando a personas”. {En línea}. {20 de diciembre de 2013}. Disponible en: (https://www.kaspersky.es/blog/ingenieria-social-hackeando-a-personas/2066/)

Es importante tener en cuenta que el ser humano es el eslabón que se puede catalogar como el punto más débil dentro de la cadena de seguridad de la información que se puede tener en una empresa, y como tal, se debe atender esta gran falla buscando formar frentes para el mejoramiento de la calidad de la seguridad.[13]

5.4 MARCO LEGAL Y NORMATIVO

El congreso de Colombia en el año 2009 aprobó la ley 1273 en la cual se expone:

5.4.1 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 y se dictan otras disposiciones.

En esta ley se fundamentan las siguientes definiciones:

Mensaje de datos: La información generada, enviada, recibida, almacenada o comunicada por medios electrónicos, ópticos o similares, como pudieran ser, entre otros, el Intercambio Electrónico de Datos (EDI), Internet, el correo electrónico, el telegrama, el télex o el telefax; [14]

Comercio electrónico: Abarca las cuestiones suscitadas por toda relación de índole comercial, sea o no contractual, estructurada a partir de la utilización de uno o más mensajes de datos o de cualquier otro medio similar. Las relaciones de índole comercial comprenden, sin limitarse a ellas, las siguientes operaciones: toda operación comercial de suministro o intercambio de bienes o

[13] ROS-MARTIN, Marcos. “Evolución de los Servicios de Redes Sociales en Internet”. {en línea} {septiembre 2009}. Disponible en: (http://www.documentalistaenredado.net/859/evolucion-de-los-servicios-de- redes-socialesen-internet/)
[14] Ley 527 de 1999. {En línea}. {18 de agosto de 1999}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276)

servicios; todo acuerdo de distribución; toda operación de representación o mandato comercial; todo tipo de operaciones financieras, bursátiles y de seguros; de construcción de obras; de consultoría; de ingeniería; de concesión de licencias; todo acuerdo de concesión o explotación de un servicio público; de empresa conjunta y otras formas de cooperación industrial o comercial; de transporte de mercancías o de pasajeros por vía aérea, marítima y férrea, o por carretera;

Firma digital: Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación;[15]

Entidad de Certificación: Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;

Intercambio Electrónico de Datos (EDI): La transmisión electrónica de datos de una computadora a otra, que está estructurada bajo normas técnicas convenidas al efecto; [16]

Sistema de Información: Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna otra forma mensajes de datos.[17]

[15] Sistema de Información de Comercio Exterior. Disponible en: (http://www.sice.oas.org/e-comm/legislation/col2.asp)
[16] El Tiempo. {En línea}. https://www.eltiempo.com/archivo/documento/MAM-1295104
[17] Alcaldía de Bogotá. {En línea}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276)

Es una normatividad que ha brindado grandes avances en seguridad para los colombianos teniendo en cuenta su campo de acción y los delitos informáticos más comunes en la sociedad.

5.4.2 Ley 1349 de 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.[18]

En donde está estipulado el objetivo de la ley como: "determinar el marco general para la formulación de las políticas públicas que regirán el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento general, el régimen de competencia, la protección al usuario, así como lo concerniente a la cobertura, la calidad del servicio, la promoción de la inversión en el sector y el desarrollo de estas tecnologías, el uso eficiente de las redes y del espectro radioeléctrico, así como las potestades del Estado en relación con la planeación, la gestión, la administración adecuada y eficiente de los recursos, regulación, control y vigilancia del mismo y facilitando el libre acceso y sin discriminación de los habitantes del territorio nacional a la Sociedad de la Información."[19]

Esta ley señala en el artículo 2 un principio orientador definiéndolo como la protección de los derechos de los usuarios. "El Estado velará por la adecuada protección de los derechos de los usuarios de las Tecnologías de la Información y de las Comunicaciones, así como por el cumplimiento de los derechos y deberes derivados del Hábeas Data, asociados a la prestación del servicio. Para tal efecto, los proveedores y/u operadores directos deberán prestar sus servicios a precios de mercado y utilidad razonable, en los niveles de calidad establecidos en los títulos habilitantes o, en su defecto, dentro de los rangos que certifiquen las entidades competentes e idóneas en la materia y con información clara,

[18] Ley 1341 de 2009. {En línea}. {30 de julio de 2009}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913)
[19] Ministerio de Tecnologías de Información. {En línea}. Disponible en: https://mintic.gov.co/portal/604/articles-8580_PDF_Ley_1341.pdf

transparente, necesaria, veraz y anterior, simultánea y de todas maneras oportuna para que los usuarios tomen sus decisiones."[20]

5.4.3 Ley 1273 de 2009. Para dar inicio, es necesario conocer que un delito informático en general se puede definir como una actividad realizada por una persona y que tiene una conducta que se define como ilícita ya sea por acción u omisión y que como consecuencia de esta se ve afectada una persona o un bien que se encuentra protegido legalmente por lo cual se pueden obtener problemas jurídicos para responder por esto, esto es lo que se define en la ley 1273 de 2009.

La ley 1273 fue aprobada el 5 de enero de 2009 por el congreso de la república de Colombia con el fin de sancionar los delitos de violación a la protección de los datos y de la información personal. Entre esto, dicha ley definió como delito informático acciones que tiene que ver con el daño informático de la información, acceso sin autorización a cualquier sistema de información, la violación de datos personales, el poner obstáculos a las redes de telecomunicación o sistemas informáticos, la suplantación de una persona en un sitio web que tenga la finalidad de obtener los datos personales de otra persona, el uso de cualquier programa o software malicioso en contra de una organización o una persona, la transferencia no autorizada de archivos o propiedades de una empresa o persona y el robo o hurto vía web de cualquier tipo. [21]

Los delitos informáticos en Colombia han sido cometidos a través de las redes de internet haciendo bullying cibernético, con la creación de falsos perfiles, realizando fraude informáticos empresas, promoviendo la pornografía infantil a través de medios audiovisuales difundidos en la red, a través del robo de la información o la interceptación de llamadas o email a personas sin ninguna

[20] Superintendencia de Industria y Comercio. {En línea}, Disponible en: http://www.sic.gov.co/sites/default/files/files/Noticias/Resolucion-71605.pdf
[21] Ley 1273 de 2009. {En línea}. {05 de enero de 2009}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492)

autorización previa por algún organismo legal o de la persona o empresa implicada.

En esta ley se describen nuevos delitos informáticos penales, esta ley denominada “De la Protección de la información y de los datos”.

A continuación, se relaciona la normatividad vigente:

La Ley 1273 de 2009 creó nuevos tipos penales relacionados con delitos informáticos y la protección de la información y de los datos con penas de prisión de hasta 120 meses y multas de hasta 1500 salarios mínimos legales mensuales vigentes.

Artículo 269B: OBSTACULIZACIÓN ILEGÍTIMA DE SISTEMA INFORMÁTICO O RED DE TELECOMUNICACIÓN. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: INTERCEPTACIÓN DE DATOS INFORMÁTICOS. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269G: SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos

legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.[22]

[22] Ley 1273 de 2009. {En línea}. {05 de enero de 2009}. Disponible en: (http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html)

6. DELITOS INFORMÁTICOS ASOCIADOS A LA INGENIERÍA SOCIAL EN COLOMBIA Y LATINOAMÉRICA

Según un artículo publicado en el portal enter.co[23], se ha podido establecer que el 97% de los ataques informáticos en Colombia no son derivados de fallas o vulnerabilidades en sistemas de información, si no, que son ocasionados con diferentes técnicas de ingeniería social que son usadas para lograr conseguir diferentes credenciales de acceso para violentar la seguridad informática e información confidencial de las personas. Por razones como estas, contar con los mejores alcances en tecnología no es importante si las personas no son conscientes de que pueden ser víctimas en cualquier momento de un ataque por ingeniería social.

6.1 PERFIL CRIMINOLÓGICO

En primer lugar, se debe tener claro lo que significa la criminología la cual hace referencia a la ciencia que se encarga de estudiar cada paso y cada comportamiento de una persona que comete algún tipo de delito, estos pueden ser uno o varios, además, también refiere a las reacciones que esta tiene enfrentando a la sociedad y como se relaciona con el delito cometido, la manera de comportamiento del delincuente, la victima que ha sufrido el hecho y el control que estos factores ejercen en la sociedad en general. Todas las anteriores son variables de análisis que pueden mostrar aspectos generales para determinar el comportamiento de un delincuente informático y de su manera de actuar para lograr los fines propuestos.

La criminología está conformada de cuatro niveles de conocimiento, el primero hace referencia a la descripción, la cual ofrece los detalles de las causas que

[23] ROMERO, Gonzalo. “La ingeniería social: El ataque informático más peligroso”. {En línea}. {25 de julio de 2016}. Disponible en: (http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/)

dan lugar a la manera de comportarse las personas con el fin de lograr cometer los delitos, de la misma manera las condiciones y las reacciones que las mismas tienen ante la sociedad en casos como estos.

La segunda hace referencia a la explicación, con esto se quiere decir que para poder llegar al nivel explicativo es necesario realizar un ordenamiento lógico de lo que se ha encontrado previamente y se definen los fenómenos delincuenciales y su vinculación las reacciones sociales.

En tercer lugar, se tiene la predicción, A través de la cual se mide el nivel predictivo y se pretende definir cuáles serían los pros y los contras del comportamiento delictivo que puede llegar a alcanzar una persona. En cuarto lugar, se tiene la aplicación, esta hace referencia al nivel aplicativo con el cual se pretende hacer una intervención directamente en cada uno de los factores delincuenciales y se establece un objetivo que busque disminuir los delitos dentro de la comunidad.

En el artículo del profesor Cesar Ramirez Luna, se define a un delincuente informático como:

> “Los delincuentes informáticos, son personas especiales (utilizan su inteligencia superior a la normal, para adquirir los conocimientos en esta materia para poder desarrollar comportamientos ilegales). Generalmente son personas poco sociables, que actúan preferentemente en la noche; son auténticos genios de la informática, entran sin permiso en ordenadores y redes ajenas, husmean, rastrean y a veces, dejan sus peculiares tarjetas de visita. Los Hackers posmodernos corsarios de la red, constituyen la última avanzada de la delincuencia informática de este final de siglo.”[24]

[24] RAMIREZ, Luna Cesar. “El perfil criminológico del delincuente informático”. P. 4. {En línea}, Disponible en: (http://www.derecho.usmp.edu.pe/centro_inv_criminologica/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf)

Un delincuente puede tener diferentes características y estilos de vida que lo conducen a cometer todas estas faltas en contra de la sociedad. Dichas características se enmarcan sobre todo en aspectos familiares, psicológicos o sociales que se han logrado adquirir a lo largo del tiempo.

El componente psicológico tiene un alto grado de importancia cuando se trata de estudiar el comportamiento de un delincuente puesto que pueden presentarse diferentes tipos de delincuentes, es por esto que para poder definir un perfil psicológico es necesario contar con un estudio profundo de la vida familiar que se tiene a lo largo de los años y de la vida social de la persona, estos aspectos pueden definir su perfil por la magnitud en importancia que pueden llegar a tener, con base en esto se estima el nivel de madurez y desarrollo como ser humano que presenta la persona o que no ha podido adquirir.

En el mundo de la informática, un delincuente no es cualquier tipo de persona, por el contrario, son personas especiales puesto que se han capacitado previamente y de esta manera hacen uso de su inteligencia para no cumplir las normas legales establecidas. Es muy común, que los delincuentes informáticos casi no socialicen con las demás personas y esto hace que ellos prefieran actuar en horas nocturnas para acceder a redes y computadores ajenos sin ningún tipo de permiso y de esta manera robar, secuestrar o dañar información fomentando la delincuencia y perjudicando a la sociedad en general.

Kevin Mitnik, un pionero en el tema con tan solo 16 años ha asegurado en diferentes ocasiones que “La información es pública, es de todos, y nadie tiene derecho a ocultarla” y cuando fue detenido sostuvo que no se creía un delincuente y decía "Un Hacker es solo un curioso, un investigador, y aquí vuestra intención equivale a enviar a un descubridor a la hoguera, como lo hacía la inquisición” [25]

[25] MORALES, Alejandro. “Delitos informáticos”. {En línea}. {04 de noviembre de 2017}. Disponible en: (http://www.monografias.com/trabajos17/delitos-informaticos/delitos-informaticos.shtml)

Una persona que comete delitos informáticos, en su mayoría de veces hace uso de un nombre ficticio para no ser rastreado ni dejar huella de los ataques que realiza, esto los hace únicos en la realidad virtual y es muy difícil seguir su paso. Unos delincuentes informáticos para realizar sus actos delictivos generalmente buscan sitios grandes, como grandes ciudades puesto que tienen sentimientos de rencor hacia las burocracias y no sobresalen en la sociedad por características específicas. También se ha podido encontrar que a estas personas no les gusta que se les compare con alguien llamado nerd, puesto que no tienen un concepto favorable de dichas personas y creen que pueden legar a ser únicos debido a su nivel de inteligencia.

Un delincuente informático es autodidacta, crea un interés particular por estudiar temas que tienen que ver con ingeniería, específicamente de sistemas, informática e inclusive electrónica, además, también pueden mostrar interés por las matemáticas, la filosofía y la física.

Además de lo anterior, se ha podido identificar que un delincuente informático se interesa por leer y por los estudios de ciencia lo cual conlleva a que tengan un alto coeficiente intelectual pues su curiosidad le facilita mucho obtener conocimiento y no se conformen con lo que tienen si no que por contrario cada vez tienen mayor deseo de seguir explorando su mundo virtual. Se ha evidenciado que, en su mayoría, un ciberdelincuente, no suelen consumir sustancias alucinógenas incluyendo el alcohol, por el contrario, su adicción se centra en pasar horas o días frente a un computador explorando las redes y el mundo virtual, este resulta siendo su mayor vicio.

Es bastante común que este tipo de personas tampoco practiquen deportes, en consecuencia, si tienen gusto por alguno de estos es muy común que lo pongan en práctica únicamente a través del televisor o de un video juego, esto porque evita tener contacto físico con las demás personas. Con esto, también tienen que

ver la manera en la que se alimentan, la mayoría de estas personas prefieren hacerlo comiendo comidas rápidas.

Actualmente, se pueden distinguir dos tipos de delincuentes informáticos:[26]

1. Se asocia con quienes tienen pleno conocimiento del uso de la tecnología con dolo en busca de cometer un delito.

2. Se asocia con quienes buscan robar información, ejecutar un delito o beneficiarse directamente del suceso y por estos motivos hacen uso de la tecnología como ayuda para conseguirlo.

Un ciberdelincuente, también se caracteriza por ser una persona que realizan actividades delictivas usando medios electrónicos como las redes sociales, los emails y el internet en general, se desenvuelven hábilmente en el entorno virtual pues este es su entorno de trabajo o ámbito de desempeño.

Para poder identificar un perfil de un ciberdelincuente, en forma general se presenta en personas con problemas familiares - sociales, por inestabilidad social - económica y por los problemas políticos y de educación.

6.2 TIPOS DE ATAQUES DE INGENIERÍA SOCIAL

En la ingeniería social los ataques pueden ser de dos tipos, unos son los ataques locales y otros son los ataques remotos. Los primeros hacen referencia a los ataques que se realizan en personas, no necesariamente con conexión de telecomunicaciones y los segundos tienen que ver con los que se realizan haciendo uso de internet y las diferentes redes de telecomunicación.

[26] DE LA CUESTA ARISMENDI, José L y PÉREZ MACHÍO, Ana I. “Ciberdelincuentes y Cibervítimas”. {En línea}. {Capítulo 3. P. 99}. Disponible en: (https://www.ehu.eus/documents/1736829/2010409/CLC+91+Ciberdelincuentes+y+cibervictimas.pdf)

El portal web, RedUSERS ha definido como ataques locales los siguientes:

6.2.1 Pretexting / Impersonate. Esta es una técnica que se puede dar de manera local o remota. Para la manera local, se puede tomar como un buen ejemplo el caso en el que una persona que trabaja en la oficina de sistemas de alguna empresa instala un software sin autorización excusándose en algún tema de daño de servicio y ganando la confianza de su víctima, luego de esto se ejecuta el programa instalado y toma el control del equipo accediendo a datos sensibles del usuario de manera remota.[27]

6.2.2 Tailgating. Este es un ataque que va directamente a la solidaridad y buena voluntad de la víctima, consiste en hacer uso de habilidades sociales para lograr el ingreso a lugares restringidos o no autorizados. El ejemplo más claro se puede dar en una empresa en donde su ingreso sea restringido a través de uso de tarjetas RFID o molinetes, en el momento de ingreso de algún empleado, el atacante usara estrategias para ganar su confianza y lograr el ingreso dejando ver que olvido su tarjeta de entrada y engañando a la víctima.[28]

6.2.3 Falla en controles físicos de seguridad. Ese es un tipo de ataque muy común en las empresas, se da por descuidos de los controles que se deben tener en el ingreso a las empresas. Como ejemplo se puede tener un atacante que llega a una empresa y la persona encargada de recibirlo no confirma el origen ni el destino de la persona entrante (atacante), de esta manera accede a las instalaciones y así mismo puede llegar a obtener información propia de la empresa de alta confidencialidad.[29]

[27] Revista de Logística. {En línea}. Disponible en: (https://revistadelogistica.com/actualidad/los-colaboradores-de-las-companias-son-el-principal-objetivo-de-la-ciberdelincuencia-en-2017/)
[28] Seguridad Informática, Gf0s. {En línea}. Disponible en: (https://gf0s.com/2016/08/05/tailgating-acceso-a-zonas-restringidas/)
[29] COtm, Cointernet, Laura Tavernier. {En línea}. Disponible en: (https://www.cointernet.com.co/blog/la-ingenieria-social-el-ataque-informatico-mas-peligroso/)

6.2.4 Dumpster Diving. Este es un tipo de ataque que consiste en aprovechar el descuido de las víctimas para revisar la basura y obtener cualquier tipo de información allí arrojada, esto se da muchas veces por que los usuarios anotan contraseñas, dejan información impresa o documentos confidenciales sin destruir que posteriormente van a la basura y muchos aprovechan dichas situaciones para acceder sin ningún tipo de contratiempo.[30]

6.2.5 Shoulder Surfing. Es más común y más sencillo de lo que parece, esta técnica consiste en observar a la víctima cuidadosamente por encima del hombro para lograr saber lo que escribe y de esta manera conocer el patrón de ingreso a su celular o las contraseñas que son ingresadas.[31]

6.2.6 Distracción. Esta técnica es también conocida como desorientar, no es ni más ni menos que distraer a la víctima para obtener información valiosa, robar un token, tomar alguna fotografía de algo importante, tomar un papel sin ser descubierto, hacer uso o extraer información de algún dispositivo de almacenamiento, etc.[32]

6.2.7 Baiting. Esta técnica consiste en hacer uso de pendrives (dispositivos de almacenamiento) con software maliciosos por medio de los cuales se hace seguimiento detallado a la víctima y se logra identificar la vulnerabilidad más acertada para ser usada en contra.[33]

[30] Portafolio, {En línea}. Disponible en: (https://www.portafolio.co/tendencias/usuarios-el-punto-debil-para-que-entren-cibercriminales-510863)
[31] Ministerio de Tecnologías de la Información. {En línea}. Disponible en: (https://www.mintic.gov.co/portal/604/w3-propertyvalue-19215.html)
[32] PISCITELLI, Emiliano. Ibid. {En línea}. Disponible en: (http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/)
[33] ESED, Welivesecurity. {En línea}. Disponible en: (https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social)

6.2.8 Phishing. Esta es una técnica que busca pescar víctimas. Para lograrlo se haces diferentes envíos de correos electrónicos con archivos adjuntos que no son más que malware o links de páginas falsas que con su uso logran tomar control del equipo de la víctima o lo que es peor buscan entablar una relación con la misma aprovechándose de sus sentimientos y pensamientos. Un buen ejemplo de esto es cuando se hace un engaño tomando la identidad de una persona mayor y ofreciendo dar dinero por bienes que supuestamente le heredara a alguien por algún tipo de favor o buen comportamiento. Para realizar estas transacciones, a la víctima se le solicitan algunos documentos personales y datos confiables los cuales son usados para hacer fraudes o solicitar créditos en entidades bancarias y solicitar diferentes servicios a nombre de la víctima la cual es la que termina siendo afectada por dichas situaciones. [34]

6.2.9 Redes sociales. Esta es una técnica con dos objetivos que son muy ambiciosos, el primero es conseguir información de la víctima y el segundo es lograr una relación con la misma.

Hoy en día, por medio de las redes sociales muchas personas difunden cada paso que dan dejando a disposición completa de cualquier atacante su vida personal y lo que realizan cada día en cada instante. Estas personas son de gran utilidad para un buscador de víctimas ya que es muy fácil acceder a su información personal pues sin querer o sin ser consientes ellos mismos están exponiendo no solo su vida personal, sino que incluso puede llegar a su vida laboral y datos confidenciales de la misma.[35]

[34] La Republica. {En línea}. Disponible en: (https://www.larepublica.co/internet-economy/colombia-entre-los-20-paises-donde-mas-se-envia-spam-2571499)
[35] El Nuevo Herald. {En línea}. Disponible en: (https://www.elnuevoherald.com/noticias/finanzas/article177012756.html)

6.2.10 Telefónicos. Esta técnica consiste en hacer uso de un teléfono para lograr técnicas de ataques como la pretexting o impersonate de forma más fácil, sencilla o segura. Kevin Mitnick fue un Hackers Telefónico que logro realizar cosas increíbles haciendo uso de un teléfono.[36]

6.3 TÉCNICAS DE APLICACIÓN DE LA INGENIERÍA SOCIAL

Se ha conocido la opinión de la ingeniera Jacqueline Tangarife, quien es la gerente de la organización Security Solutions & Education, empresa que es la representante exclusiva para Colombia de EC-Council Academia "La ingeniería social no es una técnica cuadriculada. Esta, está ligada con la malicia del atacante, así como la de la víctima. Se debe conocer que se puede hacer uso de muchas mañas y técnicas para lograr obtener o acceder a la información que se necesita: esto tiene en cuenta desde sobornos a amigos y familiares con el fin de que faciliten el acceso a la misma, hasta preguntas generales que poco a poco van dejando ver información clave, correos electrónicos que en apariencia son inofensivos que hacen preguntas sencillas y cuyas respuestas interesan a quien solicita la información". [37]

De esta manera, la ingeniería social se ha venido convirtiendo en un tipo de habilidad o arte para aprovecharse de las circunstancias de manera intencional, a su vez este refiere a las características psicológicas que tienen las personas como la confianza, la curiosidad o el miedo, las cuales generan cambios en el comportamiento de las personas.

Se ha conocido a lo largo del tiempo que la ingeniería social actúa de cuatro formas diferentes:

[36] Colombia Digital, David López. {En línea}. Disponible en: (https://colombiadigital.net/actualidad/articulos-informativos/item/8556-la-ingenieria-social-el-usuario-continua-siendo-el-eslabon-mas-debil.html)
[37] ARBELÁEZ, Ana. "Ingeniería Social: El Hackeo Silencioso". {En línea}. {19 de junio de 2014}. Disponible en: (http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/)

> La primera consiste en las técnicas pasivas, basadas en la observación y en el análisis de la víctima. Como cada caso es diferente, el éxito está supeditado al contexto en el que la persona se mueve, a través de la observación de este se logra construir un perfil psicológico tentativo que permita un óptimo abordaje. La segunda técnica utilizada es la no presencial, en la cual se recurre a los medios de comunicación como el teléfono o los correos electrónicos para intentar obtener información útil, según sea el caso. Gracias a los avances tecnológicos y a la apropiación de la tecnología en nuestra vida cotidiana, esta técnica resulta ser la más común y, al mismo tiempo, la más efectiva. En tercer lugar, están las técnicas presenciales no agresivas que incluyen el seguimiento a las personas, la vigilancia de los domicilios y la búsqueda en la basura con el fin de juntar la mayor cantidad de información. Finalmente, están los métodos agresivos que recurren a la suplantación de identidad, la despersonalización y las presiones psicológicas. Según los expertos en seguridad, la combinación de este último grupo de técnicas, junto a la explotación de las tres técnicas mencionadas en el párrafo anterior, puede ser altamente efectiva en el trabajo cara a cara entre víctima y victimario.[38]

Existen algunos pasos que se logran ejecutar en el momento en que se aplica la ingeniería social, en primer lugar, se realiza un acercamiento y de esta manera se crea un tipo de confianza. Ese primer acercamiento se puede realizar por diferentes medios siempre teniendo el cuidado necesario de que las víctimas no percaten la situación, es por eso por lo que no generan situaciones que pongan en duda el plan para ejecutar el arranque. Este es uno de los pasos más importantes pues de él depende la ejecución exitosa del plan de ataque. Dando continuidad a este, se tiene el ejercicio realizado para recopilar la información básica, esta se debe obtener de manera sutil, la víctima debe estar tan conectada con el delincuente que esta debe brindar información sin esfuerzo y la misma

[38] ARBELÁEZ, Ibid. {En línea}. Disponible en: (http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/)

será utilizada para cometer el fraude, si la información no es exacta por lo menos sirve para iniciar un proceso de pruebas.

A continuación, se hace una relación de las diferentes técnicas que son utilizadas para la realización de ataques mediante ingeniería social, se recuerda que no son aplicadas necesariamente a personas sino también a empresas, además, para lo atacantes es mucho más sencillo encontrar puntos vulnerables en las personas que en los sistemas de información que en su mayoría son equipados con estándares de seguridad por las organizaciones que los controlan:

6.3.1 Habilitación de macros. Los delincuentes informáticos usan la ingeniería social con el fin de lograr engañar o mentir a los usuarios de diferentes organizaciones y de esta manera habilita macros para que el malware que se tiene de macros entre en funcionamiento. En estos ataques se visualizan como los cuadros de diálogo que son falsos y aparecen en los documentos que se estén usando de la plataforma de Microsoft Office y llevando a los usuarios a que autoricen que las macros sean mostradas correctamente para que el contenido creado se disponga en una versión más actualizada del producto de Microsoft.[39]

6.3.2 Sextorsión. La Sextorsión son tipos de ataques por medio de los cuales los delincuentes informáticos se presentan a sus víctimas como amigos e incluso posibles amantes los cuales las logran atraer a que se realicen videos o fotos intimas, las mismas sean compartidas con ellos y posteriormente las puedan chantajear. En la actualidad estos ataques están llegando también a las empresas y no son solo contra individuos.[40]

[39] GONZALEZ, Adrian. “Las 6 técnicas más eficaces de ingeniería social”. {En línea}. {28 de mayo de 2017}. Disponible en: (https://revistaitnow.com/las-6-tecnicas-mas-eficaces-ingenieria-social/)
[40] El Mercurio, Emolo. {En línea}. Disponible en: (https://www.emol.com/noticias/Internacional/2018/07/27/914811/Sextorsion-El-delito-informatico-que-atormenta-a-usuarios-de-internet-en-diversas-partes-del-mundo.html)

6.3.3 Ingeniería social de afinidad expandida. Este tipo de ataque de ingeniería social busca formar un grado de afinidad con la futura víctima que se está contemplando para cometer el acto delictivo. Los atacantes identifican puntos de conexión como gustos que comparten por equipos deportivos, políticas, situaciones, etc. Y de esta manera avanzar más profundamente hacia las víctimas logrando obtener su confianza.[41]

6.3.4 Reclutadores falsos. Es bastante común que existan personas dedicadas a ofrecer trabajos u oportunidades extraordinarias que resulten siendo falsas para lograr obtener información que posteriormente usaran para sus fraudes.[42]

6.3.5 Pasantes viejos. Hoy en día se conocen bastantes pasantes de edad avanzada, no solo jóvenes. Estos, aprovechan el conocimiento que tienen y a su vez su alta experiencia para cometer espionaje industrial en un alto nivel. Por dicha experticia, saben de qué manera llegar a las personas, que deben preguntar y como deben actuar para encontrar información confidencial para robarla más fácilmente.[43]

6.3.6 Bots de ingeniería social. Estos ataques están siendo utilizados con el fin de infectar navegadores web, basados en esto, en el futuro se logra acceder a las sesiones de navegación y a su vez secuestrar secuestrarlas para posteriormente hacer uso de credenciales de acceso a redes sociales guardadas en el navegador y de esta manera enviar mensajes infectados a diferentes amigos y así aprovechar la información allí expuesta.[44]

---

[41] Revista It Now, {En línea}. Disponible en: (https://revistaitnow.com/las-6-tecnicas-mas-eficaces-ingenieria-social/)
[42] Azul Web, XOCHITL RODRIGUEZ. {En línea}. Disponible en: (https://www.azulweb.net/la-ingenieria-social-algunas-formas-llevarla-cabo/)
[43] Criminalista Cibernética, Hansgross {En línea}. Disponible en: (https://hansgross.com.pe/2018/04/26/evite-ser-victima-de-estafas-electronicas-reconozca-un-ataque-de-ingenieria-social/)
[44] Kapersky. {En línea}. Disponible en: (https://latam.kaspersky.com/resource-center/definitions/what-is-social-engineering)

6.3.7 Antivirus y programas con afectaciones al usuario. Se han creado antivirus y programas informáticos con malas intenciones que lo que hacen es introducir falsas órdenes a los sistemas. Así las cosas, estos falsos programan crean en los usuarios la duda de la existencia de un virus en su sistema, esto con el fin de que realicen la descarga del antivirus que generalmente resulta siendo un programa malicioso conocido como adware.[45]

6.3.8 Falsas noticias sobre personas cercanas. En la actualidad, una de las técnicas que está siendo muy utilizada es por medio del uso de las redes sociales, esto se realiza sabiendo que los usuarios son bastantes y día a día se incrementa el interés por el uso de estos medios de comunicación. Existen falsas réplicas de aplicaciones de redes sociales, un ejemplo es una réplica del Facebook, en el momento en que un usuario instala estas aplicaciones se ve totalmente expuesto puesto que con ellas se pueden enviar o acceder a mensajes como si fuesen propios.[46]

6.3.9 Portales de descarga. Esta es una técnica que está causando gran impacto, la manera en cómo se ejecuta es promocionando un software común y de confianza para el público en general. Cuando las personas quieren descargar e instalar dicho software se encuentra con que accede a sus datos personales causando grandes y graves daños.[47]

[45] JULIA, Samuel. “Las técnicas para propagar malware, cada vez más sofisticadas”. {En línea}. {10 de noviembre de 2017}. Disponible en (http://www.gadae.com/blog/las-tecnicas-para-propagar-malware-cada-vez-mas-sofisticadas/)
[46] CIO America Latina, Adolfo Manaure. {En línea}. Disponible en (http://www.cioal.com/2012/04/04/amenaza-en-facebook-promete-cambiar-la-vista-al-color-rosa/)
[47] Ondigital Magazine. {En línea}. Disponible en (http://www.ondigitalmagazine.com/2013/07/black-hat-2013-conozca-nuevos-metodos-y-tecnologias-utilizados-por-el-cibercrimen/)

6.3.10 Extensiones falsas de navegadores. Los atacantes están haciendo uso de falsas notificaciones de actualización o complementos para los navegadores, estas pueden resultar en amenazas para los usuarios y sus datos confidenciales.[48]

6.4 ATAQUES DE INGENIERÍA SOCIAL EN COLOMBIA Y LATINOAMÉRICA

El 10 de octubre de 2016, Ana Maria Luzardo publicó en el portal Enter.co un artículo en donde aseguraba que las redes sociales son un medio que expone a la sociedad a ser víctimas de ataques de seguridad informática. Para esto se refiere a:

> El pasado 2 de octubre -en el marco del Plebiscito por la Paz- varias personas expresaron en Facebook su compromiso con el país al publicar sus certificados de votación con el número de sus cédulas a la vista de todos. Algunos dirían que el número de la cédula no es tan trascendental -más si hace parte de las bases de datos de los bancos, la Registraduría General de la Nación, entre otras instituciones gubernamentales- pero no se imaginan todos los casos de fraude y suplantación que se pueden generar a partir de este dato.
>
> Si quisiéramos ahondar en más incidentes de seguridad -según una encuesta reciente realizada por ESET Latinoamérica- el 35% de los usuarios de redes sociales sufrió un incidente de malware (también conocido como código maligno o software malicioso) que puso en riesgo su intimidad. Esto quiere decir que 1 de cada 3 usuarios se infectó con algún tipo de código maligno a través de campañas de ingeniería social

[48] Taringa. {En línea}. Disponible en (https://www.taringa.net/+info/nuevos-intentos-de-secuestro-de-cuentas-de-facebook_13p1qd)

que utilizan los ciberdelincuentes para robar información, controlar el sistema infectado o adquirir las contraseñas del usuario.[49]

Esta encuesta la realizó ESET Latinoamérica a su comunidad en redes sociales durante el mes de julio, y sus resultados también evidenciaron que el 30% de las personas hicieron clic en una publicación extraña que los llevó a ser víctimas de algún tipo de engaño. Para los expertos de ESET, es habitual que los atacantes utilicen este tipo de campañas maliciosas para hacer que en los perfiles de las personas se propaguen contenidos falsos o se realicen publicaciones de manera involuntaria.

De hecho, es así como -sin necesidad de que se descargue un programa en el computador o en el celular- los ciberdelincuentes logran hacer la suscripción del usuario a servicios de publicidad que generan costos adicionales, como servicios de SMS premium.

Facebook fue -según los encuestados- la red social más visitada, y el 80% la usa para compartir contenidos. De estos contenidos, el 56.3% corresponde a fotos, videos y textos de autoría propia, mientras que un 45% tiene que ver con información personal como nombre, apellido, nacionalidad, edad, correo electrónico, estado civil, dirección, teléfono y código postal, respectivamente.

Otro de los resultados relevantes de la encuesta es que el 15% de los usuarios fue víctima de phishing, un ataque que tiene como objetivo adquirir información personal o confidencial de las personas de forma fraudulenta. El phishing es muy común a través del correo electrónico o sitios web duplicados, pero actualmente se está realizando con regularidad en otros medios como las redes sociales.[50]

---

[49] Gadae Netweb. {En línea}. Disponible en (http://www.gadae.com/blog/las-tecnicas-para-propagar-malware-cada-vez-mas-sofisticadas/)

[50] LUZARDO, Ana Maria. “35% de usuarios de redes sociales estuvo expuesto a software malicioso”. {Enter.co}. {En línea}. {10 de octubre de 2016}. Disponible en:

Teniendo en cuenta esta información, se puede observar la importancia del cuidado de los datos personales, un dato tan publico aparentemente como lo es el número de cedula está siendo usado para generar distintos tipos de fraudes los cuales afectan de diferentes maneras a las personas quienes inconscientemente revelan datos con los que un delincuente puede realizar diferentes actividades.

Otro claro ejemplo de uso de esta técnica fue publicado en el año 2015 por el periódico El Tiempo en Colombia. Aquí se señalaba “Por estos días resuena el nombre de Jaime Alejandro Solano, bautizado como el 'rey del robo de millas'. Es señalado de hurtar 5 millones de millas a clientes de Diamond Avianca. Solano acudió a la persuasión y al engaño para ganarse la confianza de sus víctimas y llevarlas a entregar sus datos de acceso a las zonas de administración de información de la aerolínea. Así, concretó movimientos delictivos exitosos basados no solo en su dominio de la computación, sino en su capacidad para manipular a las personas. Es decir, acudió a la 'ingeniería social'.” [51]

En este mismo artículo se hace una clara relación de lo que se podría definir como un primer ataque en la historia mediante el uso de la ingeniería social. Este tiene que ver con “las murallas infranqueables de la ciudad de Troya. No existía arma ni ejército capaz de romper las defensas de dicha ciudad; vencer por intermedio de la fuerza bélica era un imposible. Sin embargo, los griegos obraron con astucia y construyeron un enorme caballo de madera y lo obsequiaron, en lo que parecía ser un gesto honorable de su parte con sus enemigos, en su interior aguardaba un ejército que asoló la ciudad cuando cayó la noche. Conquistaron lo imposible por medio del ingenio y la manipulación.” [52]

(http://www.enter.co/chips-bits/seguridad/35-de-usuarios-de-redes-sociales-estuvo-expuesto-a-software-malicioso/)

[51] MEDINA, Edgar. “Ingeniería social, la razón del éxito de los ladrones digitales”. {Periódico El Tiempo}. {En línea}. {29 de junio de 2015}. Disponible en (http://www.eltiempo.com/archivo/documento/CMS-16020156)

[52] MEDINA, Ibid. {En línea]. Disponible en `(http://www.eltiempo.com/archivo/documento/CMS-16020156)

De esta manera se puede observar que la ingeniería social no es algo que haya iniciado en la época actual, sin embargo, sigue habiendo mucho por mejorar en cuanto a la prevención que debe existir en la conciencia de las personas.

Caracol Radio el 31 de agosto de 2011 publicó:[53]

> Normalmente, se relaciona el tema de los hackers con la informática y las plataformas tecnológicas, sin embargo, existe otra modalidad que se aleja de los scripts y las penetraciones de las redes, es conocida como la ingeniería social. En el marco del Congreso Interamericano de Seguridad Informática, Segurinfo, se realizó una charla llamada "Ingeniería Social: otra forma de hackear", en donde Guillermo Santos, presidente de la revista Enter.co, explicó en qué consiste esta modalidad de sustracción de información. Citando a Kevin Mitnick, famoso por haber hecho uso de la ingeniería social para cometer delitos, se podría definir a este método como "el arte de conseguir de un tercero aquellos datos de interés para el atacante por medio de habilidades sociales", en este caso, la mente de las personas es la que se debe vulnerar mediante engaños o trucos para poder obtener la información deseada
>
> Las técnicas son variadas: llamadas telefónicas en donde se hacen pasar por personas de confianza, superiores o miembros de empresas de credibilidad, como bancos y aseguradoras para sustraer información.
>
> También, están los correos electrónicos que se valen de engaños como el bloqueo de una cuenta bancaría, y certificación de algún sitio web al cual se encuentra suscrito.

[53] Caracol Radio. "Ingeniería Social: el hackeo humano". {En línea}. {31 de agosto de 2017}. Disponible en: (http://caracol.com.co/radio/2011/08/26/tecnologia/1314366240_538059.html)

> Otra forma de hacer ingeniería social es por medio del spam: supuestos e-mails con información de personalidades populares de la música, política o religión; hechos de interés común y catástrofes que, si llegan a ser abiertos o direccionados por enlaces, pueden terminar por infectar o robar información de la víctima.
>
> Sin embargo, algunas de las técnicas más exitosas incluyen el manejo de confianza de personas que suplantan o se hacen pasar por empleados dentro de una organización. En esos casos, las formas de interacción son las que determinan el éxito, ya que, si se obtiene la confianza de algún portador de información, es probable que en una conversación se termine por brindar los datos que el delincuente necesita.
>
> Por último, es necesario crear políticas de seguridad que tengan en cuenta este tipo de situaciones, y también concientizar a todos los niveles de la organización frente a la confidencialidad de la información. Se puede iniciar con acciones simples como evitar dejar a la vista datos privados, tener cuidado de quiénes pueden acceder a ciertas instalaciones y papeles, y administrar adecuadamente la basura, ya que en la mayoría de los casos memorias USB, CD's DVD's, discos duros, bases de datos de clientes y empleados, y agendas telefónicas son desechadas sin ninguna precaución.[54]

El diario el tiempo, el 17 de marzo dio cabida a un artículo titulado "Candidatos a rectoría de la U. Nacional piden garantías tras hackeo", en el mismo se puede apreciar la siguiente noticia:[55]

> El actual rector de ese claustro, Ignacio Mantilla, denunció este martes que las cuentas de correo electrónico de él y otros tres aspirantes a la

[54] Caracol Radio. "Ingeniería Social: el hackeo humano". {En línea}. {31 de agosto de 2017}. Disponible en: (http://caracol.com.co/radio/2011/08/26/tecnologia/1314366240_538059.html)
[55] EL TIEMPO. "Candidatos a rectoría de la U. Nacional piden garantías tras hackeo". {En línea}. {17 marzo 2015}. Disponible en: (http://www.eltiempo.com/archivo/documento/CMS-15416939).

> rectoría de la Universidad Nacional fueron hackeadas y usadas para enviar información maliciosa o errónea, con el fin de generar confusión.
>
> Los tres candidatos son Carlos Agudelo, Fabián Sanabria, Mario Hernández, quienes también hicieron eco de la situación a través de sus redes sociales.
>
> “Ante el hackeo de cuentas oficiales de los candidatos (…) ¿qué garantías ofrece la actual administración? (…) Debe dar garantías de seguridad informática en el proceso de designación del rector”, señaló Sanabria.
>
> El proceso de elección del nuevo rector se realizará este miércoles, entre las 8:00 a. m. y las 4:00 p. m.
>
> Del grupo de cinco candidatos que reciban el mayor apoyo de la comunidad (incluido el que reciba más votos de los estudiantes), el Consejo Superior Universitario (CSU) elegirá al nuevo rector de la universidad pública más importante del país.
>
> Se espera que el 25 de marzo se conozcan los resultados de este proceso, y que el 2 de mayo de este año el nuevo rector comience labores.

Noticias como esta, son impactantes para la sociedad puesto que los daños o asaltos por medio de ingeniería social están afectando a toda la población, incluso a la población estudiantil lo cual es grave y se debe catalogar como un delito que tiene todo para ser castigado por la ley.

Por otro lado, se tiene el no cumplimiento de la normatividad creada para evitar los delitos informáticos en cualquiera de sus aplicaciones, por ejemplo, en el ao 2014, el diario informativo El Espectador expuso a los colombianos la siguiente entrevista al juez segundo de control de garantías Alexander Díaz autor de la Ley de delitos informáticos que hoy tiene Colombia y uno de los mayores

expertos sobre nuevas tecnologías del derecho y la protección de datos en el país[56]:

> El autor de la ley que castiga dichas conductas dice que el país tiene la mejor normatividad del continente. El problema es que en el sistema judicial no la aplican bien.
>
> En medio del escándalo del hacker capturado por la Fiscalía general de la nación, acusado de interceptar correos electrónicos de integrantes de la mesa de negociación en La Habana y vinculado a la campaña presidencial de Óscar Iván Zuluaga, se ha podido evidenciar la falta de conocimientos que hay en el país frente a la legislación existente sobre los delitos informáticos. Por tal razón El Espectador habló con el juez segundo de control de garantías Alexander Díaz, autor de la Ley de delitos informáticos que hoy tiene Colombia y uno de los mayores expertos sobre nuevas tecnologías del derecho y la protección de datos en el país.
>
> ¿Existe legislación en Colombia para castigar los delitos informáticos? Claro que existe. Yo fui el que redactó el proyecto de ley de los delitos informáticos en Colombia y la que se constituyó después como la ley 1273 de 2009.
> ¿Y es suficiente esa legislación o falta algo por incorporar?
>
> Tan es suficiente y está bien hecha que fue considerada por el Congreso de la Fiadi (Federación Iberoamericana de Asociaciones de Derecho e Informática) en Santa Cruz de la Sierra, por todos los informáticos de América asociados a este organismo como la mejor ley de delitos informáticos del continente.

[56] ZULUAGA, Camila. “En busca de cura para los delitos informáticos”. El Espectador. {En línea}. {13 de mayo de 2014}. Disponible en: (https://www.elespectador.com/noticias/politica/busca-de-cura-los-delitos-informaticos-articulo-492170)

¿Tiene usted conocimiento de cuántas personas en Colombia han sido castigadas bajo esa ley?

No tengo el número exacto, pero según se me ha informado ha sido un número considerable pero no significativo de éxitos para atacar efectivamente este flagelo. No es porque no existan medios legales sino porque mis colegas, los jueces de la República y los delegados del fiscal general de la nación no entienden muy bien la tipificación de la conducta informática.

Es importante anotar que Colombia y Latinoamérica debe fortalecer sus esquemas conceptuales con respecto a los castigos que deben merecer los delincuentes informativos pues de esta manera pueden causar daños directos e indirectos a la sociedad, al país y hasta al mundo entero si no se logran los controles necesarios para evitarlo.

7. MEDIDAS DE SEGURIDAD

7.1 METODOS DE PREVENCIÓN

La manera más efectiva para evitar ser víctima de procedimientos de ingeniería social es no revelando información personal y confidencial siendo así precavidos con toda la información que se brinda a los demás especialmente a personas desconocidas. Además, se deben seguir las siguientes recomendaciones que evitan caer más fácilmente en estos procedimientos:

1. Leer a cerca de los métodos de estafa más utilizados y los nuevos, esto con el fin de estar precavidos de las estrategias que se puedan estar utilizando por parte de criminales. En el caso de las empresas, es importante buscar protección ante la identificación de cualquier riesgo que se identifique teniendo en cuenta que la información conforma el activo más importante para el cumplimiento de su misionalidad. Esto pasa también con personas, no solo con empresas, el mal uso de la información personal en las técnicas nuevas y antiguas de ingeniería social concluyen con la ejecución de estafas y delitos de los que cualquiera puede ser víctima.

2. Generar responsabilidad y sentido de pertenencia para implementar seguridad de manera más acertada. Esta es la mejor forma de contrarrestar la ejecución de delitos informáticos a través de esta metodología de ingeniería social, la concientización de las personas debe ser primordial para el autocuidado de la información y la minimización de los riesgos en materia de seguridad.

3. Capacitarse, informase y utilizar ejemplos de la vida real como método de prevención y preparación para recibir ataques. Es importante tener en cuenta todos los tipos de ataques que se han presentado hasta el

momento por medio de la ingeniera social, recibiendo estos claros ejemplos, se puede crear un modo de prevención las personas, cuando se tienen antecedentes se pueden identificar mucho más fácil si se esta siendo sujeto de recibir algún ataque de este tipo.

4. Fomentar la cultura de la seguridad de la información y la no revelación de datos personales. Realizar campañas de protección de datos es una manera muy eficaz de prevenir que la información sea accedida de manera ilegal, por eso importante el poder fomentar la cultura del cuidado de esta, esto previene ataques y ayuda a las personas a ser más cuidadosas a la hora de revelar información confidencial.

5. Tener conocimiento del tema de la ingeniería social, sus aplicaciones, sus componentes y sus afectaciones para saber a ciencia cierta al problema que la sociedad se enfrenta, en la medida en que la población tiene conocimiento de la existencia de algo, se van generando barreras de protección. Este es un tema que puede sonar común para las personas, pero es fundamental conocer que la ingeniería social existe y aún más, que existen los delitos informáticos aplicados por medio de esta.

6. Nunca brindar información que tenga que ver con usuarios y contraseñas de aplicaciones solicitados a través de algún mail o de una página web. Es importante conocer que esta información es personal e intransferible, este es el código de acceso a cualquier aplicación informática y se debe conocer que el uso indebido de usuarios y/o contraseñas puede generar faltas graves incluso para el usuario que comparte esta información confidencial. En ultimas es el directo afectado del acceso indebido que se produzca.

7. No intercambie ni comparta información recibida mediante correos electrónicos de personas que no conoce y no sabe su procedencia. Es importante tener en cuenta que siempre se debe conocer quién está

detrás de un correo electrónico, esto por que se han presentado muchos casos de cuentas falsas que se crean con el único fin de acceder maliciosamente a los datos. Solo se debe compartir información con usuarios conocidos y plenamente identificados.

8. Evitar caer en trampas en las cuales mediante alguna llamada se solicita realizar consignaciones, ofrecen beneficios, brindan recompensas demasiado jugosas, ofrecen descuentos en servicios públicos o entregan regalos, esto solicitando además complementar información como dirección, datos familiares, números de tarjetas de crédito o débito. Este esta siendo actualmente una de las mayores técnicas para el robo de dinero a personas, por eso se debe evitar siempre el brindar información confidencial o personal por vía telefónica a personas desconocidas.

9. Tener cuidado con los medios utilizados en la oficina al ingresar con un nombre de usuario y contraseña que puede ser registrada en alguna cámara, copia o acceso no deseado. Además, en el lugar de trabajo también se puede hacer uso de alguna USB infestada con virus que secuestre los archivos, para esto siempre se debe contar con antivirus que detecte cualquier intento de hurto de información. Puntualmente, es importante tener presente el reconocimiento del sitio al que se accede conociendo los mecanismos existentes de robo de información que se puedan presentar.

10. Al botar cualquier documentación a la basura se debe romper la misma o destruir de tal manera que la información contenida no se pueda leer. Esto, porque en muchas ocasiones se tienen intrusos que se encargan de buscar en la basura la información confidencial que se está depositando allí. Esto sucede sobre todos con cuentas bancarias o en oficinas donde se manejan datos de alta confidencialidad. En estos archivos basura se puede dejar huella de algún dato altamente confiable que no se debe dejar

expuesto, por lo tanto, es mejor destruir los archivos y luego si desecharlos.

11. Las contraseñas deben ser establecidas con mayores factores de seguridad, en lo posible evitar usar fechas de nacimiento, numero de documento, número de teléfono o placas de vehículo. Por el contrario, las mismas deben estar registradas con patrones de seguridad altos que incluyan caracteres alfanuméricos y caracteres especiales. Los datos visibles para los demás son los primeros en ser usados a la hora de pretender ingresar indebidamente a la información, por eso se deben evitar y lograr construir contraseñas altamente seguras y que no sean de fácil acceso.

12. Evitar compartir información laboral y delicada en sitios públicos como restaurantes, parques o lugares de integración comunitarios. Estos son muy importantes teniendo en cuenta que en las empresas se deben definir estos asuntos y no en algún lugar en que la información corra algún tipo de peligro. Para esto, se debe hacer uso de las instalaciones de esta y con esto se contrarrestaría este riesgo.

8. CONCLUSIONES

1. Con la realización se está monografía se logró evidenciar que existen muchas falencias en la sociedad para tratar los temas de seguridad de la información y de datos confidenciales, el desconocimiento de lo que significa ingeniera social es bastante grande.

2. Se logró la realización de un estudio de los delitos informáticos haciendo énfasis en los más cometidos y de los que la sociedad latinoamericana es víctima más comúnmente. Se puede evidenciar en las noticias, a manera de ejemplo que hoy en día la ingeniería social viene siendo un delito cometido con facilidad pues el desconocimiento del mismo deja ver en la sociedad una gran preocupación por las estafas de las que están siendo víctimas.

3. Se brindó un concepto claro y conciso del significado de ingeniería social y las diferentes técnicas de aplicación. Este es un punto fundamental en la elaboración de este trabajo teniendo en cuenta que es el punto de partida para contrarrestar estos ataques y concientizar en cuanto a lo referente de la protección de los datos.

4. En la actualidad los delincuentes informáticos usan técnicas cada vez más nuevas, innovadoras y que no alertan fácilmente a sus víctimas, es por eso por lo que es muy importante lograr llevar a cabo programas de capacitación a los ciudadanos para promover la prevención en cada uno de ellos y de sus familias.

5. Se puede establecer que es fundamental conocer las leyes que rigen la justicia para este tipo de delitos, en muchas ocasiones las personas no denuncian porque piensan que este tipo de delitos no tiene importancia, no son castigados por la justicia o simplemente no es fácil rastrear al

delincuente. En el presente documento se pueden apreciar el resumen de diferentes normas que llevan a una sana convivencia y contribuyen con la seguridad de personas, organizaciones públicas, entidades privadas y todo el órgano de control de un gobierno y su sociedad.

6. Se analizó el perfil criminológico de un delincuente informático, teniendo en cuenta puntos como este, se puede determinar el modo de actuar, la facilidad con la que se puede acceder a la información, el tipo de población de preferencia para atacar, el esquema con el que trabaja para lograr sus cometidos y hasta las amenazas que es capaz de producir con su actuar y pensar.

9. BIBLIOGRAFIA

ABAGNALE, Frank W. “El estafador del siglo. Revista Semana”. {En línea}. {03 de enero de 2003}. Disponible en: (http://www.semana.com/gente/articulo/el-estafador-del-siglo/56149-3)

ARBELÁEZ, Ana. “Ingeniería Social: El Hackeo Silencioso”. {En línea}. {19 de junio de 2014}. Disponible en: (http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/)

BERMÚDEZ PENAGOS, Edilberto. Ingeniería Social, un factor de riesgo informático inminente en la universidad cooperativa de Colombia. Trabajo de investigación especialista en seguridad informática. Neiva. Universidad Nacional Abierta y a Distancia. Facultad de educación, 2015. 116 p.

Caracol Radio. “Ingeniería Social: el hackeo humano”. {En línea}. {31 de agosto de 2017}. Disponible en: (http://caracol.com.co/radio/2011/08/26/tecnologia/1314366240_538059.html)

DE LA CUESTA ARISMENDI, José L y PÉREZ MACHÍO, Ana I. “Ciberdelincuentes y Cibervítimas”. {En línea}. {Capítulo 3. P. 99}. Disponible en: (https://www.ehu.eus/documents/1736829/2010409/CLC+91+Ciberdelincuentes+y+cibervictimas.pdf)

DELGADO, Javier. “Los 4 principios básicos de la Ingeniería Social”. {En línea}, {27 de agosto de 2008}. Disponible en: (http://unpocodemucho.com/los-cuatro-principios-basicos-de-la-ingenieria-social)

Editorial Tripie “Ingeniería Social: El Hackeo Silencioso”. {En línea}. {19 de junio de 2014}. Disponible en: (http://www.enter.co/guias/tecnoguias-para-empresas/ingenieria-social-el-hackeo-silencioso/)

EL TIEMPO. “Candidatos a rectoría de la U. Nacional piden garantías tras hackeo”. {En línea}. {17 marzo 2015}. Disponible en: (http://www.eltiempo.com/archivo/documento/CMS-15416939)

FICARRA, Francisco. “Los virus informáticos: Entre el negocio y el temor”. Centro internacional de estudios superiores de comunicación para América Latina. {En línea}. {junio de 2002}. Disponible en: (http://www.redalyc.org/pdf/160/16007810.pdf)

GONZALEZ, Adrian. “Las 6 técnicas más eficaces de ingeniería social”. {En línea}. {28 de mayo de 2017}. Disponible en: (https://revistaitnow.com/las-6-tecnicas-mas-eficaces-ingenieria-social/)

HACK, Story. “Ingeniería Social”. {En línea}. {22 de julio de 2013}. Disponible en (https://hackstory.net/Ingenier%C3%ADa_social)

Heraldo. “10 consejos para prevenir un ataque informático” {en línea}, {marzo 2015}. Disponible en: (http://www.heraldo.es/noticias/comunicacion/2015/03/31/diez_consejos_para_prevenir_ataque_informatico_348654_311.html)

Ingeniería social. “Ingeniería social, hackeando a personas”. {En línea}. {20 de diciembre de 2013}. Disponible en: (https://www.kaspersky.es/blog/ingenieria-social-hackeando-a-personas/2066/)

JULIA, Samuel. “Las técnicas para propagar malware, cada vez más sofisticadas”. {En línea}. {10 de noviembre de 2017}. Disponible en (http://www.gadae.com/blog/las-tecnicas-para-propagar-malware-cada-vez-mas-sofisticadas/)

LEDESMA, Cristina. “Ingeniería social – El hackeo al ser humano. Un enfoque holístico”. {En línea}. {10 de octubre de 2014}. Disponible en (http://www.magazcitum.com.mx/?p=2747#.WvZWHqTt7IU)

Ley 1273 de 2009. {En línea}. {05 de enero de 2009}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492)

Ley 1341 de 2009. {En línea}. {30 de julio de 2009}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913)

Ley 527 de 1999. {En línea}. {18 de agosto de 1999}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276)

LUZARDO, Ana Maria. “35% de usuarios de redes sociales estuvo expuesto a software malicioso”. {Enter.co}. {En línea}. {10 de octubre de 2016}. Disponible en: (http://www.enter.co/chips-bits/seguridad/35-de-usuarios-de-redes-sociales-estuvo-expuesto-a-software-malicioso/)

MEDINA, Edgar. “Ingeniería social, la razón del éxito de los ladrones digitales”. {En línea}, {29 de junio de 2015}. Disponible en: (http://www.eltiempo.com/archivo/documento/CMS-16020156)

Sistema de Información de Comercio Exterior. Disponible en: (http://www.sice.oas.org/e-comm/legislation/col2.asp)

El Tiempo. {En línea}. https://www.eltiempo.com/archivo/documento/MAM-1295104

Alcaldía de Bogotá. {En línea}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=4276)

MEDINA, Edgar. “Ingeniería social, la razón del éxito de los ladrones digitales”. {Periódico El Tiempo}. {En línea}. {29 de junio de 2015}. Disponible en (http://www.eltiempo.com/archivo/documento/CMS-16020156)

MORALES, Alejandro. “Delitos informáticos”. {En línea}. {04 de noviembre de 2017}. Disponible en: (http://www.monografias.com/trabajos17/delitos-informaticos/delitos-informaticos.shtml)

OJEDA, Cesar. “Psicología y Mente. Ingeniería social: ¿el lado oscuro de la Psicología?” {En línea}, {02 de noviembre de 2017}. Disponible en: (https://psicologiaymente.net/social/ingenieria-social-psicologia)

OSEANO-It. “La importancia de protegerse contra los ataques de ingeniería social”. {En línea}, {2014}. Disponible en: (http://www.oceano-it.es/news-individual/371/protegerse-contra-ataques-de-ingenieria-social)

PISCITELLI, Emiliano. “Edición 293 de revista USERS”. {En línea}, {04 de diciembre de 2015}. Disponible en: (http://www.redusers.com/noticias/ingenieria-social-cuales-son-los-tipos-de-ataque/)

PISCITELLI, Emiliano. “Ingeniería Social: Cuáles son los tipos de ataque”. {En línea}. {2015., 5 p}. Disponible en:

(http://www.redusers.com/noticias/ingenieriasocial-cuales-son-los-tipos-de-ataque/)

RAMÍREZ SANDOVAL, Jorge Iván; DÍAZ MARTÍNEZ, José Vicente y GARIZURIETA MEZA, Miguel Hugo. “Ingeniería Social, una amenaza informática”. {en línea}, {septiembre 2009} Disponible en: (http://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica)

RAMIREZ, Luna Cesar. “El perfil criminológico del delincuente informático”. P. 4. {En línea}, Disponible en: (http://www.derecho.usmp.edu.pe/centro_inv_criminologica/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf)

ROMERO, Gonzalo. “La ingeniería social: El ataque informático más peligroso”. {En línea}. {25 de julio de 2016}. Disponible en: (http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/)

ROMERO, Op. cit. Disponible en: (http://www.enter.co/guias/lleva-tu-negocio-a-internet/ingenieria-social/)

ROS-MARTIN, Marcos. “Evolución de los Servicios de Redes Sociales en Internet”. {en línea} {septiembre 2009}. Disponible en: (http://www.documentalistaenredado.net/859/evolucion-de-los-servicios-de-redes-socialesen-internet/)

SORIANO, Miguel. “Seguridad en redes y seguridad de la información”. {En línea}. {2017}. Disponible en: (http://improvet.cvut.cz/project/download/C2ES/Seguridad_de_Red_e_Informacion.pdf)

ZULUAGA, Camila. “En busca de cura para los delitos informáticos”. El Espectador. {En línea}. {13 de mayo de 2014}. Disponible en: (https://www.elespectador.com/noticias/politica/busca-de-cura-los-delitos-informaticos-articulo-492170)