ANÁLISIS DE LAS TÉCNICAS DE INGENIERÍA SOCIAL QUE AMENAZAN LA SEGURIDAD INFORMÁTICA DE USUARIOS DE ENTIDADES FINANCIERAS

JUAN CARLOS MALAGON LARA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTA
2023

ANÁLISIS DE LAS TÉCNICAS DE INGENIERÍA SOCIAL QUE AMENAZAN LA SEGURIDAD INFORMÁTICA DE USUARIOS DE ENTIDADES FINANCIERAS

JUAN CARLOS MALAGON LARA

Proyecto de Grado – Monografía presentado para optar por el título de
ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Director de Curso
KATERINE MARCELES VILLALBA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2023

NOTA DE ACEPTACIÓN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Ciudad., Fecha sustentación

DEDICATORIA

Con cariño dedico este trabajo a mis hijos, que con su ternura y alegría me apoyan en todos los pasos de mi vida, que sin saber son quienes sostienen mi vida, gracias por su compañía y la alegría que le dan a mi vida, mirar esas caritas es lo que me motiva a crecer, trabajar y superarme días tras día, de igual modo agradezco a mi madre por su apoyo, amor y consejos; Sé que sus oraciones me acompañan en todo momento.

AGRADECIMIENTOS

Agradezco primeramente a Dios, por permitirme seguir capacitándome; Gracias a la Universidad Nacional Abierta y a Distancia UNAD, por el acompañamiento constante en las actividades académicas, a los tutores que con sus accesorias apoyan los procesos necesarios para superar este logro.

CONTENIDO

Pág.

TABLA DE ILUSTRACIONES

Pág.

GLOSARIO

ATAQUES: para este caso los; ataques informáticos. Son el intento mal intencionado y orquestado, que realizan una o más personas con el objetivo de causar daño o dificultades en una red o sistema informático. Logrando obtener de la red información valiosa y sensible.[1]

Un **ataque informático** tiene como objetivo acceder a los servidores y equipos informáticos, por medio de la introducción de virus o archivos malware, para afectar su funcionamiento, produciendo daños y extraer información sensible de personas y empresas.

MITIGACION: la mitigación de riesgos es el proceso por el cual se diseñan y desarrollan opciones y acciones que, al momento de ser implementadas, reducirán los efectos negativos, la probabilidad de que un evento en particular ocurra y mejorara las posibilidades.[2]

MITIGAR: es ejecutar medidas de prevención dirigidas a reducir los riesgos existentes. Con la mitigación se asume que en muchas ocasiones no es posible, controlar o impedir en totalidad la ocurrencia de daños y sus consecuencias, sino más bien estos son reducidos a niveles aceptables y factibles, en el desarrollo del plan de mitigación se busca disminuir las pérdidas y daños que ocurrirían con la incidencia de una amenaza informática.[3]

INTERACCION: encuentro que se lleva a cabo de manera, recíproca entre dos o más, personas, objetos, agentes, fuerzas, funciones , etc. La interacción es la esencia de la comunicación, en ella se quiere expresar algo en concreto, a través de la palabra y del lenguaje corporal. [4]

---

[1] ECURED.Ataque informático. [En Línea]. s. f- [14 de noviembre de 2021]. Disponible en:https://www.ecured.cu/Ataque_inform%C3%A1tico

[2] ESCUELA EEUROPEA DE DERECHO. Mitigación de riesgos. [En Línea]. s. f-[14 de noviembre de 2021].Disponible en: https://www.escuelaeuropeaexcelencia.com/2021/06/mitigacion-de-riesgos-proceso-de-3-pasos-para-hacer-frente-al-riesgo/

[3] CASTIBLANCO, Fernando. OVIEDO, Luis. Análisis de riesgos informáticos. [En Línea]. Junio de 2016-[18 de octubre de 2022].Disponible en: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2660/Trabajo%20de%20grado.pdf?sequence=1&isAllowed=y

[4] REAL ACADEMIA ESPAÑOLA. Interacción. [En Línea].s.f-[14 de nov de 2021].Disponible en: https://dle.rae.es/interacci%C3%B3n

CONFIANZA: la confianza es la convicción o esperanza concreta que alguien tiene de algo o de otro individuo. También se trata de la suposición con la que cada individuo obra con vigor y ánimo[5].

La confianza puede verse reflejada en varias cosas; la seguridad en el ser mismo, la ilusión de que algo evolucione según las expectativas, o en la familiaridad que se da entre los seres humanos ya sea por amistad, por parentesco y que parte de un afecto reciproco.

BIOMETRIA: estudia los métodos automáticos para el reconocimiento de forma única en los humanos apoyados en uno o varios rasgos conductuales o rasgos físicos propios; La «autentificación biométrica» o «biometría informática", En las tecnologías de la información es el estudio de técnicas matemáticas y estadísticas en base a los rasgos físicos o conductuales de un individuo, para su autentificación, es decir, "verificar" su identidad[6]

PERPETRAR: "ejecutar o llevar a cabo un delito o acción grave".[7]

Perpetrar indica el hecho de hacer o efectuar algo que constituye un delito, por lo general que representa gravedad.

HACKER: individuo con habilidades y conocimientos en informática que se dedica a encontrar fallos de seguridad en sistemas informáticos,

algunos hackers cuentan con la capacidad de introducirse en los sistemas informáticos más sofisticados, ocasionando modificación en la información existente [8]

El Hacker se caracteriza por ser una persona con amplios conocimientos en tecnología, puede ser electrónica, informática, o de comunicaciones, esta se mantiene en constante actualización de información y conoce muy bien todo lo relacionado con programación y sistemas complejos; es un profesional que se inclina a investigar todo lo relacionado con cadenas de datos encriptados y busca las oportunidades de acceder a cualquier tipo de 'información segura[9].

CONCIENTIZACION: conjunto de acciones que se relaciona con la toma de conciencia sobre una determinada situación, estas acciones buscan mostrar

---

[5] Julián Pérez Porto y María Merino. Publicado: 2009. Actualizado: 2021. Definiciones: Definición de confianza (https://definicion.de/confianza/)

[6] EDUCALINGO. Biometría [en línea].s.f.[14 de noviembre de 2021]. Disponible en <https://educalingo.com/es/dic-es/biometria>. Nov 2021 ».

[7] REAL ACADEMIA ESPAÑOLA. Perpetrar. [En Línea]-[14 de noviembre de 2021].Disponible en: https://dle.rae.es/perpetrar

[8] OXFORD. Hacker. [En Línea]-[20 de nov de 2021].Disponible en: https://languages.oup.com/google-dictionary-es/

[9] FLORES; Carlos. Tipos de Hackers. [en línea].s.f-[18 de octubre de 2022].Disponible en: https://ns2.elhacker.net/descargas/manuales/Hacking%20y%20Seguridad%20informatica/06.%20Tipos%20de%20hackers%20(Articulo)%20autor%20Carlos%20Alberto%20Flores%20Quispe.pdf

una verdad y/o hacer comprender las consecuencias de algunas decisiones tomadas. Concientizar es ahondar en el conocimiento de un tema en particular.[10]

FRAUDE: engaño por lo general de carácter económico cuya intención es conseguir un beneficio propio, que por otra parte deja a alguien perjudicado[11]
Con el fraude se comete una acción contraria a la verdad y a la rectitud, que ocasiona graves daños a la persona contra quien se comete.

VICTIMAS: una víctima es aquella persona que sufre un daño o perjuicio, que es producido por la acción u omisión, ya sea por culpa de otro individuo, o por fuerza mayor[12].

[10] PORPATO, Monica.Significado de Concientizar. [En Línea].s.f-[20 de noviembre de 2021].Disponible en: https://quesignificado.com/concientizar/
[11] OXFORD. Fraude. [En Línea].s.f-[22 de noviembre de 2021].Disponible en: https://languages.oup.com/google-dictionary-es/
[12] PEREZ;Porto,Definicion de víctima,[en línea].7 de octubre de 2010-[16 de noviembre de 2021].Disponible en: https://definicion.de/victima/

RESUMEN

Actualmente la tecnología hace parte del diario vivir, se ha convertido en una necesidad para hacer distintas actividades desde el entorno digital, como realizar trámites bancarios, ingresar a clases virtuales, hasta hacer compras *On- Line*, han facilitado múltiples tareas que antes consumían gran parte del tiempo.

Pero desafortunadamente no todo es bueno el aumento de estas actividades digitales también ha generado el aumento de amenazas de ataques cibernéticos, sobre todo el aumento de ataques de ingeniería social, que son un tipo de ataque aún más complejo ya que los atacantes utilizan más que los sistemas y redes; ellos atacan con las "fuerzas persuasivas", logrando así sus víctimas suministren información confidencial sin darse cuenta del engaño.

En Colombia el sector de la banca está altamente amenazado por los ataques de ingeniería social, por tal motivo este documento pretende analizar las características de las técnicas de ingeniería que se realizan a usuarios de entidades financieras que son los mayormente afectados por este tipo de ataques [13]; es fundamental reconocer las características de las técnicas de ingeniería social para concientizar a los usuarios de las amenazas existentes, y tomar medidas pertinentes que minimicen el riesgo de ser blanco de algún tipo de ingeniería social.

[13] SEMANA. ¿Qué están haciendo los bancos para protegerse de los ataques cibernéticos? [En Línea]. 14 de abril de 2022-[22 de marzo de 2023].Disponible en: https://www.semana.com/mejor-colombia/articulo/que-estan-haciendo-los-bancos-para-protegerse-de-los-ataques-ciberneticos/202200/

INTRODUCCION

Con frecuencia se escucha hablar de múltiples ataques a entidades financieras que en consecuencia afectan a miles de personas en el mundo, poniendo en riesgo la estabilidad y confianza en los sistemas de información y en las entidades financieras. Pero no todos los ataques efectuados a este sector son específicamente por sistemas informáticos, existe una técnica aún más compleja de identificar la “Ingeniería Social”, que es capaz de realizar sus ataques sin necesidad de sofisticados equipos informáticos; los delincuentes que utilizan este tipo de técnicas hacen uso de la manipulación y el engaño, ganando la confianza de sus víctimas para así obtener información de alta calidad con la que pueden acceder a cuentas bancarias.

En la presente monografía se ha recopilado y analizado información de la web y de distintos repositorios educativos con el fin de analizar las técnicas de ingeniería social que son llevadas a cabo para atacar a usuarios de entidades financieras, se describirán los conceptos más relevantes a fin de comprender el tema de Ingeniería Social, identificando las distintas técnicas utilizadas para este fin y así mismo las estrategias que pueden utilizarse para salvaguardar la información de las manos inescrupulosas, minimizando los riesgos y amenazas ocasionados por este tipo de ataques.

1 DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La ingeniería social es un tema que ha despertado el interés de varios investigadores que buscan alertar sobre las técnicas que son utilizadas para persuadir a usuarios de diferentes entidades; a continuación, algunos trabajos que han analizado las metodologías de ingeniería social.

Un primer trabajo por David Berenguer[14] Serrato estudiante de Seguridad de Tecnologías de la información y la comunicación propone un Estudio de metodologías de Ingeniería social, cuyo objetivo es familiarizarse con los conceptos de ingeniería social, detallar los métodos utilizados, descubrir qué tipo de información pueden obtener y cómo esta es utilizada para obtener beneficios; basado en su metodología de búsqueda y de síntesis de la información encontrada en libros, videos en información en la web. Detalla en su tesis las diversas metodologías de ingeniería social; como conclusiones ha llegado que:

- ✓ La ingeniería social es una técnica difícil de identificar por lo que es importante la protección de la información.
- ✓ La herramienta con la que cuentan las empresas para prevenir los ataques de ingeniería social es la concientización.
- ✓

El segundo trabajo Benavides Eduardo; Fuertes Walter y Sánchez Sandra; Estudiantes de la Escuela Politécnica Nacional, Propone realizar una "Caracterización de los ataques de *phishing* y técnicas para mitigar los ataques"[15] realiza su trabajo a través de una revisión sistemática de la literatura; El objetivo de este trabajo es proveer a los usuarios finales y a otros investigadores, una visión de los tipos de ataques de *Phishing* existentes y de cómo estos pueden ser mitigados. Para esto, realizan una revisión sistemática de la literatura, para caracterizar y clasificar los diferentes tipos de ataque de ingeniería social, y posteriormente, exponen y clasifican los medios por los que estos ataques pueden ser mitigados, que van desde la concientización al usuario, hasta la utilización de técnicas de *Machine Learning y Deep Learning., phishing* establecidos.
Determinaron como hallazgos importantes, que los vectores más comunes de ataques de *Phishing* son los de *Spoofing Email* y de *Spoofing Website*. Los medios de mitigación más efectivos para *Zero Day en phishing*, son mediante los algoritmos

[14]BERENGER, David. Estudio de Metodologías de Ingeniería Social. [En Línea]. Junio de 2018-[10 de noviembre de 2021].Disponible en:http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf
[15] Benavides Eduardo; Fuertes Walter y Sánchez Sandra. Estudio de las técnicas de ingeniería social. [En Línea]. s.f. [10 de noviembre de 2021]. Disponible en: file:///C:/Users/user/Downloads/admin,+11%20(1).pdf

tradicionales *Machine Learning* y mediante *Deep Learning*. Recalcan la importancia de la concientización.

Un tercer documento revisado en Vía LIBRE, REVISTA ESTUDIANTIL, escrito por Alberto Cruz Cruz y Flagler Sierra Viasus. Estudiantes de Administración de Empresas. Proponen como título de su artículo "Uso y seguridad de la información de clientes en las empresas y/o entidades financieras de Colombia "[16]; En su redacción describen hechos y tipos de ataques, definen la ingeniería social; Sugieren estrategias para evitar ser víctima de estos ataques; como conclusiones determinan:
Las empresas, los clientes y proveedores de tecnologías de información (TIC), tendrán que tener más responsabilidad, aumentando su rigurosidad, siendo más exigentes en aspectos como documentación y creación de software.
Es importante la creación de guías sencillas para la educación de usuarios de internet.

- ✓ La ingeniería social no es un tema fácil de mitigar y contrarrestar, debido a la cantidad significativa de técnicas para lograr este delito.

Por otro lado, EDNA ROCIO PLAZAS GARCIA, 2018, Propone una monografía "INGENIERIA SOCIAL EN LAS EMPRESAS COLOMBIANAS"[17] como metodología de investigación sugiere realizar los pasos de una investigación científica. En su trabajo expone las técnicas de ingeniería social y sugiere estrategias de prevención y riesgos por estos ataques; establece como conclusiones:

- ✓ Logró determinar que existen muchas falencias en las empresas colombianas frente a la seguridad de la información.
- ✓ Se estableció que el personal de una organización es el eslabón más débil y son más vulnerables a un ataque de Ingeniería Social a través de sus técnicas.
- ✓ Las organizaciones colombianas que más padecieron de ataques de ingeniería social en los últimos años, son las pertenecientes al sector bancario, por el flujo de usuarios e información que estas manejan.
- ✓ Los usuarios finales deben tomar conciencia y adoptar mejores prácticas a la hora de utilizar los recursos tecnológicos a su cargo
- ✓ Los ataques de ingeniería social realizados en los últimos años a las empresas colombianas han venido evolucionando; ahora los atacantes han mejorado sus estrategias diseñando imágenes o *iframe* utilizan en un ataque de *phishing.*

[16] CRUZ Alberto, SIERRA Flagler. Uso y seguridad de la información de clientes en las empresas y/o entidades financieras de Colombia. [En Línea]. s.f. [12 de noviembre de 2021]. Disponible en: http://www.unilibre.edu.co/bogota/pdfs/2018/revista_via_libre_10-8.pdf#page=51

[17] PLAZAS, Edna. Ingeniería Social En Las Empresas Colombianas. [En Línea].2019. [13 de noviembre de 2021]. ¿Disponible en:https://repository.unad.edu.co/bitstream/handle/10596/18704/1094921881.pdf?sequence=1&isAllowed=y

Lic. Gabriela Victoria Musso[18], 2019 propone una investigación de “Las Técnicas de Ingeniería Social y su incidencia en la seguridad de las organizaciones actuales” realiza una mirada de los ataques desde lo técnico y lo social, de las que pueden ser víctimas los recursos humanos de la organización y por ende y aún más importantes la información que estos poseen y generan.
En el desarrollo de su investigación muestra, el desarrollo de las técnicas utilizadas por los Ingenieros Sociales, los métodos más utilizados, el tipo de información que puede obtenerse y cómo es utilizada por estos delincuentes.
El objetivo principal de su trabajo, fue proporcionar información sobre la ingeniería social, generando conciencia y conocimiento sobre el fraude informático, explicando los tipos de ataques realizados por medio del uso de las Tecnologías de la Información y de la Comunicación, a los que están expuestos el personal de distintas organizaciones en el momento de operar, algún tipo de dispositivo electrónico, usuario, clave y/o sistemas empresariales.

Realiza algunas recomendaciones como:

- ✓ Ampliar el conocimiento sobre seguridad de la información a todas las personas operarias de dispositivos digitales, sin importar el cargo que desempeñen, realizando un análisis integral de las interacciones técnicas y sociales que se presentan comúnmente.
- ✓ Describir las principales formas de evitar un ataque de ingeniería social, mediante campañas de concientización.
- ✓ Elaborar material de apoyo para el personal de seguridad informática de la organización, cuyo objetivo sea orientar y ayudar en la toma de decisiones respecto seguridad de la información se refiere.

Dado a lo anterior, expone como conclusiones:

- ✓ Cada uno de los integrantes debe considerar la seguridad de la empresa a la que pertenece como una parte integral de sus responsabilidades individuales.
- ✓ Observa limitaciones en el desarrollo del trabajo, relacionadas a la variedad de información que se encuentra sobre las técnicas expuestas.

[18]MUSSO, Gabriela. Las Técnicas de Ingeniería Social y su incidencia en la seguridad de las organizaciones actuales.[En Línea].2019-[12 de noviembre de 2021].Disponible en: http://bibliotecadigital.econ.uba.ar/econ/collection/tpos/document/1502-1753_MussoGV

1.2 FORMULACIÓN DEL PROBLEMA

La información es considerada el activo más valioso de las organizaciones hoy en día, motivo por el cual organizaciones [19](gubernamentales, educativas, financieras, etc.), implementan planes, procesos y medidas de seguridad para proteger su información, como *firewalls*, sistemas de acceso biométricos, circuitos de cámaras de seguridad, cajas fuertes, entre otros; medidas que aportan seguridad a los sistemas informáticos de manera significativa.

Pero, hay un recurso al que las organizaciones no le han prestado la suficiente atención, la "mente humana", esté recurso guarda información muy sensible y representa un reto asegurar la información existente en la cabeza de los seres humanos; no son suficientes los candados físicos o lógicos que se implementen para proteger un activo, cuando se le da acceso a una persona se genera un riesgo humano que es muy vulnerable a la ingeniería social.

[20]Actualmente los seres humanos son el eslabón más vulnerable dentro de la cadena de custodia de activos informáticos, de nada sirve implementar los sistemas de seguridad de la información más costosos y sofisticados, ni adquirir *firewall* y *software* de seguridad de la información, si no se tiene personal con la formación necesaria para darle seguridad y acceso a los equipos que utiliza.

Las prácticas de manipulación de ingeniería social[21] son especialmente peligrosas, ya que las victimas de estas técnicas de ingeniería social no se percatan de que están siendo manipuladas sino hasta que es demasiado tarde y los delincuentes ya han logrado obtener los datos confidenciales que esperaban; utilizando esta información privada de los usuarios para hacer robo de identidad, extorciones y fraudes.

Los delincuentes detrás de[22] la ingeniería social no escatiman en poner manos en los datos más sensibles de los usuarios, aprovechando todas las interacciones en la red ya que estos datos son una verdadera mina de oro para sus propósitos, es importante resguardar la información de los dispositivos porque en ellos se guarda todo tipo de información relevante como claves de seguridad de acceso, información bancaria e información personal de suma importancia. Es por este motivo que se

[19] SANDOVAL, Edgar. Ingeniería Social: Corrompiendo la mente Humana. [En Línea].s.f-[10 de septiembre de 2021].Disponible en: https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

[20] PICHINCHA. Ataques de Ingeniería Social. [En Línea].s.f-[12 de septiembre de 2021].Disponible en:https://www.pichincha.com/portal/blog/post/ataques-ingenieria-social

[21]BODNAR,Danielle.¿Que es Ingeniería Social Y cómo evitarla?.{En Línea}.29 de octubre de 2020-[15 de octubre de 2021].Disponible en: https://www.avast.com/es-es/c-social-engineering

[22]ADVIRSORS.Riesgos y Amenazas de la Ingeniería Social. [En Línea].27 de febrero de 2018-[14 de septiembre de 2021].Disponible en:https://www.gb-advisors.com/es/riesgos-y-amenazas-de-la-ingenieria-social/

hace importante reconocer las técnicas de ingeniería social existentes identificando como se llevan a cabo este tipo de ataques, con el objetivo de concientizar a todos los usuarios de los riesgos que este tipo de amenazas trae para la seguridad de la información y así mismo tomar las medidas pertinentes para lograr minimizar estos ataques.

De aquí el interrogante que se plantea para empezar con el desarrollo de esta monografía.

¿Cuáles son las características de las técnicas de Ingeniería social que afectan a usuarios de Entidades Financieras?

2 JUSTIFICACIÓN

La nueva era de la tecnología y el creciente uso de las tecnologías de la información[23], propiciada por los efectos de la pandemia del COVID 19 ha provocado que miles de personas en todo el mundo realicen cada vez más actividades en el entorno digital, nuestra vida diaria gira en torno de actividades cada vez más digitalizadas, servicios médicos, actividades educativas, trámites gubernamentales, servicios de emergencia, pagos y transacciones financieras entre un sin número de actividades son realizadas en la actualidad a través del ámbito digital; a su vez los ciudadanos se encuentran más expuestos a amenazas y riesgos cibernéticos. En la actualidad tanto empresas como personas están expuestas al latente riesgo de un delito informático; por lo tanto, es imprescindible identificar las amenazas de estos ataques informáticos y unir esfuerzos para contrarrestar su impacto.

Sectores como la banca y la salud son los principales blancos de ciberataques [24]". Las amenazas van desde descargas no deseadas y troyanos que permiten tomar el control de los dispositivos, hasta la explotación de vulnerabilidades, pasando por el robo de información crítica."; en[25] el territorio colombiano la mayoría de los bancos están trabajando por mejorar su seguridad, debido al creciente uso de la banca móvil, que pone en riesgo su infraestructura TI. Por tal motivo se centra este estudio en analizar las técnicas de Ingeniería social, las características de las diferentes técnicas que son llevadas a cabo a usuarios de entidades financieras que son el eslabón más débil dentro de la estructura de seguridad de la información; es clave que todos los usuarios, conozcan los riesgos a los que se encuentran expuestos y de esta manera poder combatir la ciberdelincuencia, que por el desconocimiento y la habilidad de los atacantes en trabajar la mente de sus víctimas, se está en riesgo de caer en redes de la ingeniería social.

El presente estudio pretende mostrar las diversas técnicas que utilizan los delincuentes informáticos para aplicar ingeniería social y servir de documento referencial para futuros estudiantes de ciencias de tecnologías de la información que al investigar encuentren un documento fácil, claro de entender que permita a los lectores reflexionar y tomar las medidas pertinentes para minimizar los riesgos producto de la ingeniería social.

[23] BID. Mensajes Institucionales. [En Línea].Julio de 2020-[6 de septiembre de 2021].Disponible en: Reporte
[24] AETECNO.Banca y salud los principales blancos de ataques.[En Línea].6 de marzo de 2020-[17 de septiembre de 2021].Disponible en:https://tecno.americaeconomia.com/articulos/banca-salud-e-ingenieria-social-son-los-principales-blancos-de-los-ciberataques-en
[25]PLAZAS, Edna.Op. Cit., p.78

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar las características de las Técnicas de Ingeniería Social que amenazan la seguridad informática a usuarios de entidades financieras, mediante recopilación y revisión de información académica y científica, con el propósito de reconocer como son efectuados estos ciberataques y así implantar las mejores estrategias y metodologías de prevención a este tipo de ataques.

3.2 OBJETIVOS ESPECÍFICOS

- ✓ Examinar las características de las técnicas de ingeniería social que aquejan la seguridad informática de los usuarios de entidades Financieras en Colombia.

- ✓ Establecer los riesgos y amenazas de la ingeniería social en su intento por quebrantar la seguridad digital a través de la recopilación y revisión de fuentes de consulta bibliográfica, dispuesta en los repositorios autorizados para este fin.

- ✓ Proponer estrategias y métodos de seguridad de la información que se pueden implementar para proteger y minimizar los riesgos ocasionados por los ataques de ingeniería social.

4 MARCO REFERENCIAL

4.1 MARCO TEÓRICO

4.1.1 Riesgos de seguridad en el sector financiero. El sector financiero lo componen un conjunto de organizaciones, entidades, medios y mercados que facilitan, a el país y sus habitantes el movimiento de dinero.
El sector financiero es el encargado de canalizar los recursos de los habitantes para ofrecer y crear servicios de ahorro, crédito, financiación, con los que se satisfagan necesidades generales y particulares de las empresas y los individuos.
La conforman establecimientos como los bancos, cooperativas financieras, compañías de financiamiento, administradoras de pensiones, fiduciarias, compañías de seguros, bolsas de valores, entre otros, dirigidas por el Banco de la República, quien dictamina las políticas monetarias y crediticias del país. Dicho sistema tiene ciertas responsabilidades, con las que promueven un sano desarrollo económico del país; Entre las principales responsabilidades del sector financiero esta garantizar la seguridad de la información o datos de las personas, en el uso todos sus canales digitales.[26]

4.1.1.2 Seguridad bancaria. Las empresas del sector financiero han tenido que realizar una transformación digital, donde se elaboran novedosas campañas y métodos de protección a los activos, los clientes y su información. La protección de la tecnología y la información en el sector financiero es una prioridad; Desde la llegada de internet, el sector bancario ha hecho frente a la ciberdelincuencia, hasta el día de hoy donde el creciente uso de las operaciones digitales se ha intensificado por obra de la pandemia de COVID 19.
En la seguridad bancaria las instituciones financieras implementan procesos, herramientas, protocolos y métodos para proteger, la información, el patrimonio y demás activos de usuarios y colaboradores. Las metodologías y herramientas utilizadas para enfrentar posibles delitos y errores en la red, están compuestos por sistemas de seguridad y protección, electrónicos o físicos y por capacitaciones que son aplicadas en todas las áreas y son puestas en conocimiento a todos los colaboradores de la institución, con el propósito de salvaguardar la información dispuesta en la red.[27]

4.1.1.3 Riesgos en la seguridad bancaria. Los avances tecnológicos y los riesgos y amenazas que ha tenido que enfrentar el sector por la prestación de sus servicios

[26] BANCOLDEX.Que es el sistema financiero colombiano. [en línea]. s. f- [28 de octubre de 2022]. Disponible en: https://www.bancoldex.com/sabe-que-es-el-sistema-financiero-colombiano-1630
[27]DocuSign Contributor.Los 3 principales riesgos contra la seguridad bancaria. [en línea].11 de septiembre de 2020- [28 de octubre de 2022]. Disponible en:https://www.docusign.mx/blog/seguridad-bancaria

financieros, ha hecho que la seguridad bancaria tenga una evolución progresiva, ya que los perfeccionamientos de modalidades delincuenciales han golpeado severamente los servicios que la banca ofrece a sus clientes.[28]
Gran parte de los esfuerzos que realiza la seguridad bancaria está enfocada en proteger, la falsificación de credenciales, el robo de identidad y los accesos digitales; Entre los principales riesgos y amenazas del sector bancario se encuentra[29]:

Ataques denegación de Servicio. Llamado también "atasco en autopista", aquí el acceso a los servidores de la entidad se ve bloqueada por masivas peticiones de acceso o por el uso masivo del mismo. Este tipo de ataque es realizado comúnmente por piratas informáticos; la manera de contrarrestar este ataque es mediante un *software* de monitoreo de tráfico, que redirige, rastrea y resguarda la red de este tipo de peticiones.

Ransomware: es un *malware* malicioso que se ha popularizado en los últimos años, se habla que cada 15 segundos en el mundo un *malware* ha producido un ataque, obteniendo el control de equipos o dispositivos y el contenido y accesos que hay allí. La seguridad bancaria debe innovar sus procesos con el objetivo de delimitar los accesos que ponen en riesgo los fondos bancarios.

Ingeniería inversa de las apps. La ingeniería inversa de las apps no es otra cosa que la clonación que realiza la ciberdelincuencia a apps bancarias, para utilizarlas como mecanismo de *phishing*, suplantando la identidad bancaria, y así robar datos de acceso, por medio de mensajería, emails y otras formas de comunicación.[30]

Estos riesgos son solo los principales desde donde se desglosan una cantidad de amenazas que es conveniente conocer para implementar las medidas de seguridad adecuadas para cada caso.

4.1.1.4 Protección y seguridad bancaria. Los bancos y demás entidades financieras deben renovar la tecnología, fortaleciendo la detección y prevención de fraudes cibernéticos, las entidades financieras juegan un papel importante con sus campañas de sensibilización y educación financiera, a los usuarios para que por medio de estos mecanismos se conozcan los riesgos existentes en los canales digitales. El reconocer los riesgos funciona como blindaje de protección ante posibles ataques, continuación algunas medidas de seguridad bancarias:

Uso de claves únicas de acceso. Las claves de accesos a los sitios web deben ser únicas, es decir no generar una misma clave para entrar al banco y para ingresar a una red social; Estas claves deben ser complejas de descifrar utilizando

[28] OEA. Estado de la Ciberseguridad en el Sector Bancario en América Latina y el Caribe. [en línea]. S.f- [31 de octubre de 2021]. Disponible en:https://www.oas.org/es/sms/cicte/sectorbancariospa.pdf
[29] DocuSign Contributor. Op. Cit.,
[30] Ibid.,

combinación de números, letras, mayúsculas y minúsculas, también deben contener un carácter especial, con la ayuda de un generador de contraseñas es posible que las claves sean mucho más seguras.

Uso de firma electrónica. La firma electrónica es una buena medida de seguridad ya que cada firma contiene un paquete de datos único, que solo puede ser autorizado por el titular, demostrando su autenticidad y aprobación. Con el uso de la firma digital, transacciones en la web como pagos, autorizaciones y transacciones son más seguros de realizar.

Autenticación en dos pasos. La autenticación en dos pasos o autenticación en doble factor es el método habitual utilizado por los bancos donde se realizan preguntas de seguridad luego de generar un token o ingresar una clave, en esta autenticación las repuestas a las preguntas de seguridad las tiene únicamente el usuario.[31]

La seguridad bancaria cuenta con variados métodos de protección de la información, es importante seguir las recomendaciones enviadas por los bancos, desconfiar de correos y mensajes de texto sospechoso y siempre actuar con serenidad, verificando la autenticidad de correos, mensajes y supuestas llamadas de urgencia.

4.1.2 Ingeniería social como vector de ataque a usuarios del sector financiero. Los vectores de ataque son los medios y formas utilizadas por los piratas informáticos, a través del cual puede introducir o trasmitir malware a su víctima, con la finalidad de obtener beneficios claramente económicos.
Los vectores de ataque a la ciberseguridad, encuentran las falencias y debilidades en los equipos ofimáticos, las aplicaciones, en el personal que las maneja y en la red. Es este el motivo por el que implementar técnicas de seguridad informáticas, para cada posible ataque es vital en la cadena de seguridad de la información.

4.1.2.1 Tipos de vectores en la seguridad informática. En la actualidad existen distintos vectores de ataque con los que realizan accesos no autorizados a la red, pero se pueden establecer dos como los principales**:**

Vectores de ataque pasivos: Este tipo de arremetida como su nombre lo indica es un atentado pasivo utilizado comúnmente en ataques de ingeniería social donde su accionar pasa casi desapercibido y si bien busca ganar acceso a los sistemas no

[31] Ibid.,

los afecta seriamente, es usado en técnicas como el *phishing, sniffing* y *Spear phishing.* [32]

Vectores de ataque activos: Los vectores de ataques activos al contrario de los pasivos, si alteran los sistemas informáticos, bloqueando por completo la red y modificando información sensible, en este tipo de ataque se hace uso de *ransomware, malware* y ataques DDoS.

4.1.2.2 **Vectores más usados por la ciberdelincuencia.** Los ataques a la ciberseguridad cada día son más sofisticados por lo que las organizaciones deben contar con soluciones que se adapten a los constantes cambios y a la avanzada de estos ataques. Entre los vectores más usados por la ciberdelincuencia se encuentran:

Correo electrónico: El uso común y recurrente de los correos electrónicos lo convierte en el principal vector de ataque que ha sido utilizado por décadas para enviar correos no deseados, practicar la suplantación de identidad, y enviar códigos maliciosos.

Navegación por internet. Es efectuado cuando por descuido o trampa se descargan códigos maliciosos mientras se hacen búsquedas en internet.

Ataques de fuerza bruta. En los ataques de fuerza bruta el ciberdelincuente, accede a fácilmente a cuentas de organizaciones que están trabajando de forma remota y ha generado nombres de usuarios y contraseñas genéricas fáciles de vulnerar.

Aplicaciones web. Las aplicaciones web son un vector de ataque porque haciendo uso del robo de identidad la ciberdelincuencia hace uso de la información que estas muestran para engañar a los usuarios.

Explotación de vulnerabilidades. Los *"exploits*" son uno de los vectores más utilizados, ya que las malas prácticas y la falta de actualizaciones en la red por parte de los departamentos informáticos de las organizaciones permiten encontrar huecos en la seguridad que son fáciles de vulnerar**.**

***Endpoint* o dispositivos finales.** Este tipo de vector es llevado cabo desde puestos fijos de trabajo donde por medio de una memoria USB o un disco duro extraíble se introduce *malware* en un computador para infectar una red LAN.[33]

[32] IN CIBERSEGURIDAD. ¿Qué son vectores de ataque en ciberseguridad? [en línea] .4 de abril de 2022- [1 de noviembre de 2021]. Disponible en: https://www.optical.pe/blog/vectores-de-ataque-ciberseguridad/
[33] Ibid.,

Salvaguardar la información de los diversos vectores de ataque de ingeniería social, y estar atentos a los constantes cambios de la tecnología son retos complicados pero necesarios para minimizar el impacto producto de estos ataques.

4.2 MARCO CONCEPTUAL

4.2.1 Ciberseguridad. Conjunto de medidas, métodos, elementos, y equipos que trabajan encaminados a inspeccionar, vigilar y mantener la seguridad informática en las organizaciones o espacios virtuales. [34]

En la ciberseguridad trabajan en conjunto, los recursos, las políticas, los conceptos de seguridad, las prácticas idóneas, las directrices, las salvaguardas de seguridad, métodos de gestión del riesgo, acciones, investigación y desarrollo, seguros y tecnologías que pueden ponerse en práctica buscando la disponibilidad, integridad, autenticación, confidencialidad, cuya finalidad es proteger los activos y usuarios de una organización en el ciberespacio.[35]

Por otro lado, los ciberataques amenazan con modificar, destruir, y acceder a información confidencial; con el objetivo de extorsionar a los usuarios o interrumpir el normal funcionamiento de los negocios. Por lo que se hace vital, proteger los sistemas, las redes, y los programas de ataques virtuales; esto se consigue con buenas prácticas en ciberseguridad.

Fijar planes de emergencia, denegaciones y autorizaciones de servicio, fijar planes, políticas de seguridad de la información, establecer horarios de funcionamiento, y disponer de todos los protocolos necesarios que fomenten un nivel de seguridad informática óptimo, son prácticas de ciberseguridad que se deben establecer e implementar con el objetivo de minimizar los riesgos en la infraestructura informática y a la información que esta posee[36].

4.2.2 Medidas de aseguramiento empleando la seguridad informática. Este es un tema fundamental para la protección de la información de cualquier organización, y persona por lo que es importante reconocer las clases de seguridad existentes que permitan tomar acciones en cada una de ellas.
Existen cuatro áreas principales que contempla la seguridad informática:

[34]OXFORD,Languages.Definicion de Ciberseguridad.[En Línea].s.f-[20 de septiembre de 2021].Disponible en: https://languages.oup.com/google-dictionary-es/
[35] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Política general de seguridad Nacional.[En Línea].11 de abril de 2016-{22 de septiembre de 2021}.Disponible en:https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf
[36] CISCO. ¿Qué es Ciberseguridad?. {En Línea}. s. f-{20 de septiembre de 2021}.Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

- ✓ **Confidencialidad:** En esta área solo pueden acceder a los recursos tecnológicos, datos e información los usuarios autorizados.
- ✓ **Integridad**: Los datos podrán ser modificados únicamente por los usuarios autorizados.
- ✓ **Disponibilidad:** Debe existir disponibilidad de los datos para los usuarios siempre que sea necesario.
- ✓ **Autenticación:** Verificar que la comunicación sea real y se estén comunicando quienes realmente se quieren comunicar.

Existen tres tipos de Seguridad Informática:

- ✓ Seguridad **de *hardware***

Este tipo de seguridad se aplica especialmente a la protección de elementos físicos con el objetivo de evitar intromisiones y amenazas. Cuando se realiza seguridad de hardware se pretende encontrar vulnerabilidades existentes en los equipos desde su fabricación, hasta los dispositivos que tienen contacto con los equipos como lo son dispositivos de entrada y salida.
Las herramientas más utilizadas en la seguridad de hardware son los servidores intermedios (proxy) o cortafuegos, entre los menos comunes están los módulos de seguridad de hardware (HSM) los cuales suministran claves criptográficas para el cifrado, el descifrado y la autenticación. Estas herramientas para la seguridad de hardware controlan de manera profunda el tráfico de red, ofreciendo una seguridad más potente, lo que la convierte en una seguridad más robusta y con filtros adicionales de seguridad.

- ✓ Seguridad **de *software***

Este tipo de seguridad da protección al *software* contra ataques realizados por hackers, protegiendo además defectos de diseño, mal manejo de los mismos, casos de desbordamientos de buffer, y errores de implementación entre otros.
La seguridad de software protege el software y las aplicaciones de amenazas externas como virus o ataques maliciosos. La herramienta más utilizada en este tipo de seguridad es el antivirus que dispone de actualizaciones automáticas que ayudan a encontrar virus nuevos. También son herramientas los cortafuegos, filtros anti spam, software para filtrar contenidos y publicidad no deseada.

- ✓ Seguridad **de red**

En la seguridad de red se trabajan actividades dirigidas a salvaguardar su uso por medio de la protección de datos de red que conserven su fiabilidad, seguridad e integridad y prevenir así que la información sea robada o distorsionada.
Entre las amenazas más comunes en la red están:

- ✓ Gusanos Virus, y caballos de Troya
- ✓ *Software* espía y publicitario
- ✓ Ataques de *hackers*
- ✓ Ataques de denegación de servicio

- ✓ Ataques de día cero, también llamados ataques de hora cero
- ✓ Robo de identidad
- ✓ Intercepción o robo de datos

Los componentes de seguridad de red incluyen antivirus y *antispyware*, cortafuegos, sistemas de prevención de intrusiones y redes privadas virtuales.[37]

4.2.3 Tipos de ciberamenazas. En la ciberseguridad existen tres tipos de amenazas:[38]

Los ciberataques: Esta amenaza involucra la recopilación de información con fines políticos.

El ciberterrorismo: En esta amenaza los delincuentes buscan debilitar los sistemas electrónicos con el objetivo de causar pánico o temor.

El delito cibernético: En el delito cibernético los delincuentes son agentes individuales o grupos que atacan a los sistemas con el objetivo de obtener beneficios financieros o causar interrupciones.

Los atacantes cibernéticos utilizan distintas técnicas para acceder a las redes empresariales y personales; Estos son algunos tipos de ciberataques:

- ✓ ***RANSOMWARE***

El *ransomware* es un *software* malicioso que al ingresar en el equipo informático le permite al *hacker*, bloquear el dispositivo desde una ubicación remota. También otorga al delincuente permisos para encriptar los archivos haciendo que los usuarios pierdan el control de toda su información y sus datos almacenados.

El *ransomware* tiene un método de propagación en forma de troyano, lo que quiere decir, se propaga infectando el sistema operativo. Un ejemplo de cómo se lleva a cabo este ataque es descargando un archivo o explotando una vulnerabilidad del software. En este tipo de ataques el ciberdelincuente, que ha cifrado los archivos del sistema operativo inutilizando el dispositivo, suele pedir un rescate a cambio de quitar la restricción a los documentos. [39]

- ✓ ***WHALING***

Los ataques *whaling*, centran sus ataques en un perfil de alto directivo, como Ceos o CFOs. Su objetivo como los demás ataques, es robar información vital, a aquellos que ocupan puestos altos en una empresa ya que ellos suelen tener acceso ilimitado a información confidencial. En la mayoría de estos casos el delincuente hace que su víctima realice transferencias electrónicas de alto valor.

---

[37]INFOSECURITY.Ciberseguridad.[En Línea].s.f-[5 de octubre de 2021].Disponible en: https://www.infosecuritymexico.com/es/ciberseguridad.html

[38] LATAM,Kaspersky.¿Que es Ciberseguridad?.[En Línea].s.f.-[5 de octubre de 2021]. https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

[39]HERNANDEZ,Camilo.¿Qué tipos de ciberataques existen?[En Línea].9 de julio de 2020-[1 de octubre de 2021].Disponible en: https://incp.org.co/que-tipos-de-ciberataques-existen/

A este ataque le llaman «caza de ballenas» que hace referencia al tamaño del ataque, estos ataques son en teoría más fáciles de detectar, por lo que los responsables de seguridad informática de la empresa deben trabajar en minimizar efectividad de este pirateo.

- ✓ ***MALWARE***

Este ataque funciona con un código que es creado para irrumpir sigilosamente un sistema informático. Un *malware* daña, invade o deshabilita los ordenadores de los, sistemas informáticos logrando tener el control de las operaciones.
El *malware* tiene por objetivo sacar dinero al usuario de forma ilícita. Aunque este no puede dañar el *hardware* de los sistemas, sí puede cifrar y robar datos, secuestrando funciones básicas de un ordenador, así como espiar su actividad sin que nadie lo note.

- ✓ **DESCARGAS AUTOMÁTICAS**

Este tipo de amenaza busca propagar *malware* por medio de descargas automáticas, es uno de los tipos de ataques más común entre los tipos de ataques de ciberseguridad. Las descargas automáticas utilizan páginas web inseguras e implantan un script malicioso en el código HTTP o PHP en una de ellas. Este script instala *malware* directamente en el dispositivo del usuario que visite el sitio web. También puede coger la forma en un *iframe* que direcciona al usuario a un sitio controlado por los atacadores. Estos ataques son llamados «descargas automáticas» porque no necesitan ninguna acción por parte del usuario. Solo tiene que visitar dicha web para ser blanco de este ataque.

- ✓ **INYECCIÓN DE CÓDIGO SQL**

La amenaza inyección de SQL es un tipo de ciberataques encubierto en el que un *hacker* introduce un código propio en un sitio web con el fin de debilitar las medidas de seguridad e ingresar a datos protegidos. Una vez dentro el delincuente controla la base de datos del sitio web y secuestra la información de los usuarios. [40]

4.2.4 Ingeniería Social. La Ingeniería Social es la acción que comete el ciberdelincuente con el objetivo de manipular a una persona a través de técnicas psicológicas y habilidades sociales para cumplir metas específicas.
En la ingeniería social su objetivo es obtener información confidencial a través de técnicas de manipulación de usuarios legítimos. Es una técnica utilizada por ciertas personas con poca ética profesional, para extraer información, accesos y hasta privilegios de los sistemas de información, teniendo como resultado, ataques

[40]BELCIC,Iván.¿Que es inyección SOL?[En Línea].22 de septiembre de 2020-[3 de octubre de 2021].Disponible en: https://www.avast.com/es-es/c-sql-injection

similares a un ataque a través de la red, omitiendo sigilosamente toda la infraestructura diseñada para combatir programas maliciosos. Este tipo de ataque es más eficiente, debido a que es más difícil de suponer y prever.
El principio que sustenta la ingeniería social es el que en cualquier sistema "los usuarios son el eslabón débil." [41]

4.2.5 Tipos de vectores de ataque de Ingeniería Social. Los ataques a la seguridad son llevadas a cabo de diversas maneras y formas. Se desarrollan fuera de la red, realizando una llamada telefónica o, en ocasiones hasta con la visita inesperada de un supuesto funcionario a la oficina solicitando alguna información de la empresa.
Entre los ataques de Ingeniería Social se encuentran:

PHISHING
El *Phishing* es un ataque de Ingeniería Social en el que el atacante simula ser una empresa, persona, o institución para que la víctima confíe y suministre información como números de cuentas bancarias y claves de acceso Esta técnica es aún más peligrosa cuando el objetivo determinado es un funcionario que tiene acceso a diferentes sistemas dentro de su organización.

SPEAR PHISHING
El Spear *phishing* es un ataque de tipo ingeniería social en el que se envían mensajes electrónicos de forma específica a organizaciones o personas con el objetivo de instalar malware en el equipo de cómputo de la víctima y así robar información sensible y valiosa que podrá ser utilizada con fines maliciosos.
Este tipo de mensajes parecen venir de una fuente confiable; son capaces de utilizar la imagen del banco, los logos de las tiendas; Por lo que los usuarios no prestan mucha atención a la legitimidad de un mensaje que parece provenir de una entidad verdadera. Estos mensajes están creados específicamente para engañar a las víctimas re direccionándolas a sitios web falso con grandes contenidos de *malware*. [42]

BAITING
El *Baiting* es un ataque de ingeniería social en el que el atacante utiliza un dispositivo; por ejemplo una USB, infectándola con un *malware* y dejándola en un lugar fácil de encontrar; en estos dispositivo suelen utilizar palabras como “importante” o “confidencial”, que provocan la curiosidad de sus víctimas, estas al

[41] UNAM.Ingenieria social corrompiendo la mente humana. [En Línea].s.f-[20 de nov de 2021].Disponible en:https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana
[42] ESYSTEM.Ingeniería social.[En Línea].s.f-[15 de octubre de 2021].Disponible en: https://www.esystems.com.co/ingenieria-social-que-es/

conectar el dispositivo a sus equipos instalara de manera inmediata un *software* malicioso a su PC, el *Baiting* es un tipo de ingeniería social en el que no hay relación directa con una red.

VISHING O PRETEXTING

El *Vishing o Pretexting* es un tipo de ataque más actualizado de *phishing,* también conocido como *phishing* de voz; esta técnica consiste en suplantar un número de teléfono de forma que parezca legitimo; los atacantes se harán pasar por amigos o familiares, y utilizaran historias en las que probablemente un tío, primo o amigo está en la cárcel y al que hay que cancelar una significativa suma de dinero para que este salga del aprieto**.**

SMISHING

El *Smishing* es un ataque que utiliza los dispositivos móviles para enviar mensajes de texto, en los que se les pide a los usuarios realicen alguna acción que inmediatamente los llevan a vínculos maliciosos donde pueden extraer datos importantes, como números telefónicos. [43].

DUMPSTER DIVING

El *Dumpster Diving* es un ataque de ingeniería social en el que el atacante explora la "basura", es decir la papelera de reciclaje en la que muchas veces se tira información importante, el atacante tiene como objetivo encontrar información valiosa, utilizando *softwares capaces* de juntar estos *puzzle*, con los que puede obtener los datos de correo electrónico, claves y contraseñas, números telefónicos, diseños, planos, borradores de proyectos del usuario y así poder pasarse por él en la red.

TECNICAS: Como técnica se define a la forma en que un conjunto de procesos y procedimientos, intelectuales o materiales, es aplicado en una tarea específica, con base en el conocimiento de una ciencia o arte, para obtener un resultado determinado.[44] **Técnica** es el conjunto de reglas, acciones, procedimientos, normas, acciones y protocolos que tiene como objetivo alcanzar un resultado determinado y efectivo, ya sea en el área de la informática, la educación, el deporte, las ciencias, el arte o en cualquier otra actividad.[45]

[43] LISA,Institute.Guia Practica Ingeniería Social.[En Línea].8 de mayo de 2020-[17 de septiembre de 2021].Disponible en: https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social

[44] SIGNIFICADOs.COM. "Técnica". [En Línea].s.f-[17 de octubre de 2021].Disponible en:https://www.significados.com/tecnica/

[45] OXFORD LANGUAGES. Técnica. [en línea]. S.f – [17 de octubre de 2021]. Disponible en: google.com/search?q=definicion+tecnica&oq=definicion+tecnica&aqs=chrome..69i57j0i512l9.5615j1j7&sourceid=chrome&ie=UTF-8

TACTICAS: "Según la real academia de la lengua española, la táctica es el "Método o sistema para ejecutar o conseguir algo.", es decir, la forma en que se va a desarrollar o ejecutar un algo para conseguir un fin, u objetivo. [46]"

SEGURIDAD DE LA INFORMACION: "La Seguridad de la Información[47], según ISO27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información y los datos importantes para la organización, independientemente del formato que tengan, estos pueden ser: Electrónicos, En papel, Audio y vídeo, etc."

AMENAZAS: Acciones que traen consecuencias negativas en el interior de la entidad, y a los usuarios; se denominan amenazas a las fallas, a los ingresos no autorizados a los virus y los desastres ocasionados por fenómenos físicos o ambientales. [48]:

DELITO INFORMÁTICO: "Conducta ilícita que debe ser sancionada por el derecho penal, consiste en aquella acción indebida que se hace en cualquier medio informático para llevar acabo delitos comunes, conductas inapropiadas, falta de éticas con el fin de causar daños en la información."[49]

4.3 MARCO HISTÓRICO

Es común hablar sobre vulnerabilidades de *software* que permiten a los atacantes obtener información confidencial por medio de accesos no autorizados; en los seres humanos se puede decir que las versiones de estas brechas de seguridad son nuestras emociones, las reacciones en las personas después de un acontecimiento aterrador son primero actuar y luego pensar; "vulnerabilidad" que es aprovechada por la ingeniería social para lograr ataques exitosos[50].

El termino de Ingeniería social fue empleado en ciencias políticas teniendo un doble sentido, uno hace referencia a influir en las relaciones o acciones sociales en la

[46] GERENCIE.COM.Que es táctica. [En Línea].27 de noviembre de 2020-[8 de octubre de 2021].Disponible en:https://www.gerencie.com/diferencia-entre-tactica-y-estrategia.html
[47] ISO,Tools.¿Que significa Seguridad Informática?[En Línea].21 mayo de 2015-[10 de 0ctubre de 2021].Disponible en:https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/
[48] CORDERO,William.IMPLEMENTACION DE TECNICAS DE INGENIERIA SOCIAL EN LA INSTITUCION EDUCATIVA TECNICA DE PANQUEBA.[En Línea].2018-[12 de octubre de 2021].Disponible en:https://repository.unad.edu.co/bitstream/handle/10596/22690/91532860.pdf?sequence=1&isAllowed=y
[49] Ibid.
[50]NORTON.Que es la ingeniería social.[En Línea].s.f-[6 de septiembre de 2021].Disponible en: https://co.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

población de un país o región, y el otro se referencia a la manera de imponer programas de transformaciones sociales.[51]

En el año 1894 el término de ingeniería social comenzó a utilizarse con un ensayo difundido en Francia del filántropo y empresario holandés J.C. Van Marken, pero esta expresión recibió su mayor impulso en EE.UU. por medio del libro "Social *Engineering"* del reformista social W.H. Tolman; donde se exponía como idea central que no había en las empresas una función social ("algo así como los departamentos de recursos humanos de hoy"), por lo que el ingeniero social tenía una función de mediar entre la organización y el trabajador para resolver los conflictos. [52]
En 1945 Karl Popper implementó el término. "el principio de Popper se basaba principalmente en el supuesto de que las personas pueden ser optimizadas al igual que la maquinaria" [53]. En los años de 1970, los descendientes de Popper ensancharon su teoría para incluir algunos tipos de engaños psicológicos. Pero, su objetivo inicial no era el robo de información, sino persuadir a la gente a una mejor interacción y a una mayor toma de conciencia en materia de salud. Esto, en efecto, aplicaba manipulación, pero su objetivo era diferente al que existe hoy en día.

A pesar del significado negativo que el término tiene en la actualidad, se puede decir que todo esfuerzo de una organización pública o privada cuyo objetivo sea cambiar el comportamiento puede considerarse como ingeniería social. Se puede decir que los medios de comunicación, la religión y la política con sus campañas buscan comportamientos específicos en las personas por lo que el término de ingeniería social aquí es definitivamente aplicable.

En la actualidad el termino de ingeniería social es empleado para referirse a la forma como los atacantes pueden sacar provecho de otro; por este motivo se ha estudiado el tema y se encuentra diversos documentos en la web con el propósito de concientizar a los usuarios de diferentes entidades sobre el impacto que esta tiene sobre las personas.

[51] LEDESMA, Cristina.Ingenieria social.[En Línea[.s.f-]8 de septiembre de 2021].Disponible en:https://www.magazcitum.com.mx/index.php/archivos/2747#.YZkQuWDMKM8
[52]BERENGER,David.Estudio de Metodologías de Ingeniería Social.[En Línea].Junio de 2018-[10 de noviembre de 2021].Disponible en:http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

[53]GDATA.Que es realmente la ingeniería social.[En Línea].s.f-[15 de noviembre de 2021].Disponible en: https://www.gdata.es/guidebook/what-actually-is-social-engineering

4.4 MARCO LEGAL

En Colombia existen leyes por medio de las cuales son condenados y castigados aquellos que comentan delitos informáticos y pongan en riesgo la seguridad de la información y la comunicación; de igual forma existen leyes que protegen a los usuarios financieros. A continuación, una pequeña descripción de la normatividad vigente:

Ley 1273 De 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".[54]La expedición de esta ley en Colombia, fue el punto de partida en la lucha contra los delitos informáticos, buscando así reglamentar y castigar todas las acciones consideradas delitos informáticos, salvaguardando la información y los datos. La Ley está organizada en dos capítulos, el primero menciona "los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos" y el segundo "los atentados informáticos y otras infracciones".[55]

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, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"[56]

La presente ley tiene como objetivo desarrollar el derecho constitucional dando a las personas la legitimidad para conocer, actualizar y rectificar la información que se haya reunido sobre ellas en los diferentes bancos de datos, y otorgar derechos, libertades y garantías por medio de la constitución, en la que la recolección, tratamiento y circulación de datos personales sea regulada, así como también el derecho a la información ya establecido en la Constitución Política, especialmente en relación con la información suministrada en entidades financiera e información crediticia, de servicios, comercial y la enviada de otros países.

LEY 1341 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"[57]

---

[54] SECRETARIA DEL SENADO. Ley 1273.[En Línea].20 oct de 2021-[17 de noviembre de 2021].Disponible en:http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

[55] MENDEZ,Alejandro.Estudio de Metodologías de Ingeniería Social.[En Línea].Diciembre de 2018-[12 de noviembre de 2021].Disponible en:http://openaccess.uoc.edu/webapps/o2/bitstream/10609/90305/6/amendezcarTFM12189memoria.pdf

[56]SECRETARIA DEL SENADO.[En Línea].Ley 1266 de 2008-[13 de noviembre de 2021].Disponible en:http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

[57] ALCALDIA DE BOGOTA.Ley 1341 de 2009.[En Línea].s.f-[17 de nov de 2021].Disponible en:https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

Con esta ley se formulan las políticas públicas que se tendrán en cuenta en el sector de Tecnologías de la información y las comunicaciones, reglamentando su ordenamiento en general, la protección del usuario, el régimen de competencia, el uso eficiente de las redes tecnológicas, el uso eficiente del espectro radioeléctrico, así mismo como se tendrá en cuenta la autoridad del estado en relación con la planeación, la adecuada administración y vigilancia de los recursos, suministrando el fácil y libre acceso a las tecnología de la información y la comunicación de todos los habitantes de territorio nacional.

LEY ESTATUTARIA 1581 DE 2012. "Por la cual se dictan disposiciones generales para la protección de datos personales"[58]La importancia de esta ley radica en la protección y salvaguarda de la información personal, suministrada en las diferentes bases de datos evitando el uso indebido de esta por parte de las diferentes entidades públicas o privadas; el cumplimiento de esta ley está bajo el decreto 1377 de 2013, en la que se determinan mecanismos de protección de datos de los usuarios.

LEY 1328 DE 2009. "Por la cual se dictan normas en materia financiera, de seguros, del mercado de valores y otras disposiciones"[59]
El Objetivo y aplicación de la presente ley tiene como prioridad fijar los principios y normatividad que rigen la protección de los usuarios financieros y su relación con las entidades vigiladas por la Superintendencia Financiera de Colombia, sin perjuicio de otras disposiciones que contemplen medidas e instrumentos especiales de protección. Se entiende como consumidor financiero, todo individuo que sea consumidor en el sistema financiero, asegurador y del mercado de valores.

[58] DEPARTAMENTO DE LA FUNCION PÚBLICA. Ley estatutaria 1581 de 2012.[En Línea].s.f-[18 de noviembre de 2021].Disponibleen:https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981
[59] DEPARTAMENTO DE LA FUNCIONPUBLICA. LEY 1328 DE 2009.[En Línea].s.f-[20 de nov de 2021].Disponible en:https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36841

5 DESARROLLO DE LOS OBJETIVOS

5.1 DESARROLLO DE OBJETIVO 1: CARACTERÍSTICAS DE LAS TÉCNICAS DE INGENIERÍA SOCIAL QUE AQUEJAN LA SEGURIDAD INFORMÁTICA DE LOS USUARIOS DE ENTIDADES FINANCIERAS EN COLOMBIA.

Un ciberataque tiene como objetivo vulnerar la seguridad de la manera más rápida y con el menor costo posible, para ello los delincuentes atacan a quienes son llamados el eslabón más débil dentro del esquema de seguridad de la información las “personas”. Existen diversas formas como las personas son víctimas de la ingeniería social; los ciberdelincuentes juegan con algunos elementos de los principios de la ingeniería social con los que ganan la confianza y el respeto de su víctima. Son características de las técnicas de ingeniería social:

5.1.1 Principios básicos de la ingeniería social. Existen seis (6) principios básicos en la teoría de la influencia y la persuasión, del Dr. Robert Cialdini, escritor del libro “*Influence: The psychology of persuasión*” teoría en la que se basa la ingeniería Social, estos principios son:[60]

Reciprocidad: Las personas por naturaleza son seres recíprocos con sus actos. Si otra persona ofrece algo, se quiere ofrecer algo también. Si por el contrario alguien los trata mal, existe la tendencia a responder de la misma manera. Es un instinto social muy de la naturaleza, y por ende, fácilmente manipulable.[61]

Urgencia: Es el principio más clásico entre los clásicos; aquí se presentan expresiones como ¡Aproveche esta oferta! ¡Hasta fin de existencias! ¡Durante los próximos cinco minutos…! Es una de las consignas comunes de las ventas. La mayoría de los ataques de ingeniería social, principalmente los de Hunting, atraen a las víctimas por medio de la urgencia. Utilizan engaños diciendo a sus víctimas, por ejemplo: Tienen 24 horas para consignar cierto dinero para ayudar a un familiar que está en apuros. Comparte ahora mismo este artículo entre todos tus contactos de Facebook y ganarás un súper premio.[62]

Consistencia: El ser humano es un ser de costumbres. Le gusta cumplir cuando da la palabra, se inclina más en cumplir que en no hacerlo. El caso de ingeniería social más utilizando en este principio es aquel en el que un jefe pide realice ciertas tareas, aunque entre ellas haya una que parezca “rara”; terminará por hacerla, brindando a el criminal el acceso a información muy importante de la organización.

---

[60] IGLESIAS,Pablo.Los Principios Básicos De La Ingeniería Social.[En Línea].s.f-[16 de noviembre de 2021].Disponible en:https://www.pabloyglesias.com/mundohacker-ingenieria-social/

[61] Ibid.

[62] Ibid

Confianza: Este es el principio más simple de todos, está enfocado en la simpatía que se crea entre las personas, las defensas bajan cuando la otra persona cae bien o está alineado con los mismos intereses. Se reacciona positivamente a lo que pida una persona simpática y agradable.[63]

Autoridad: El principio de autoridad describe que se suele creer que tienen mucho más poder las personas que ostentan títulos académicos y muestran amplia experiencia, se accede a las pretensiones de personas que muestran dicho poder y experiencia.

Validación social: Por naturaleza los seres humanos son seres sociales en busca de la aprobación de los demás. Por ejemplo: si en un correo electrónico alguien nos pide realizar algo raro, es posible que se piense bien primero. Pero si en esa misma conversación hay varios conocidos más (por ejemplo trabajadores de la misma compañía), que no tienen inconvenientes, se entenderá que no hay ningún problema y se acatarán las normas, vengan de quien vengan.[64]

5.1.2 Técnicas habituales de ingeniería social. Se pueden dividir en dos los tipos de ataques de ingeniería social esto depende del número de interacciones que utilizan los ciberdelincuentes:

Hunting

En este tipo de ataque se necesita una única comunicación y buscan afectar al mayor número de usuarios. Son usados comúnmente en campañas de *phishing,* como los realizados contra entidades energéticas o bancarias. Por ejemplo:
Campañas con correos fraudulentos, que suplantan compañías como bancos, redirigiendo la victima a una página falsa para que suministre datos personales allí. Estos ataques también son utilizados con el objetivo de realizar una infección por *malware*, como las que se llevaron a cabo para realizar ataques de *ransomware*: Por ejemplo:

- ✓ Falsos documentos de Excel que adjuntan códigos maliciosos.
- ✓ Falsas facturas enviadas por correo que infectan el equipo.

Farming

En el ataque tipo *Farming* el delincuente necesita realizar varias comunicaciones con sus víctimas hasta lograr su objetivo u obtener la mayor cantidad de información posible. Un ejemplo de este tipo de ataque son los que buscan infundir miedo en las víctimas por medio de supuestos videos privados o futuros ataques contra su empresa.[65]

[63] Ibid
[64] Ibid.
[65] Ibid

5.1.3 Tipos de ingeniería social. La Ingeniería Social es un acontecimiento muy amplio con diferentes tipos de técnicas de ataques que pueden utilizarse para engañar a una persona.

Dentro de estas actividades de ingeniería social existen dos grupos desde donde se empieza dicha clasificación: ataques personales y ataques escalables.
Reconocer las técnicas más comunes utilizadas en la ingeniería social, es la mejor manera de prevenir y protegerse de un posible ataque de ingeniería social. La ilustración a continuación muestra ataques de ingeniería social comunes que son utilizados por los ciberdelincuentes.[66]

Figura 1. Tipos de Ingeniería Social.

Fuente: LISA INSTTITUTE.Guia contra la ingeniería social.[imagen].Ataques de ingenieria social.Lisa institute 2020.[consultado:20 de octubre de 2021].Disponible en: https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social

En la ingeniería social los delincuentes utilizan sus habilidades sociales, con el objetivo de conseguir información personal, mediante el engaño a sus víctimas obteniendo así información de cuentas bancarias, números de tarjetas de crédito o información confidencial de empresas y sus sistemas informáticos.

66 : LISA INSTTITUTE.Guia contra la ingenieria social.[En Línea].s.f-[14 de octubre de 2022].Disponible en: https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social

Dentro de las técnicas de ingeniería social se clasifican los tipos de ingeniería social que son utilizados para cometer fraude a los usuarios. Los tipos de ingeniería social están basados en:[67]

Basada en personas: Este tipo de ingeniería social involucra la interacción con las personas, por lo general por teléfono. El atacante dice ser una persona autorizada y legitima, interactúa con las personas para obtener información sensible, por ejemplo: se hace pasar por personal de la entidad financiera. Esta práctica fraudulenta es llamada como *Vishing.*

Basada en computadores: Los atacantes haciendo uso de la tecnología realizan búsqueda de la información necesaria para sus ataques, por ejemplo: por medio de correos electrónicos que parecen ser de la organización u organizaciones legítimas y que contiene *links* a sitios maliciosos donde se solicitan datos sensibles de las personas. Esta última técnica de engaño es comúnmente conocida como *phishing.*[68]

Mediante el desarrollo de apps maliciosas: Este tipo de ingeniería social imita aplicaciones populares que al momento de ser descargadas van infectar los dispositivos, también funcionan como *links* a sitios maliciosos por medio de mensajes de texto SMS, y para así obtener información sensible de los usuarios y organizaciones.[69]

5.1.4 Vías de ataque de ingeniería social. El ciberdelincuente hace uso de sus conocimientos informáticos y de su destreza para no ser detectado, para realizar actos ilegales o facilitar los delitos a través de redes, datos, sitios *web*, sistemas y tecnologías, infringiendo así las leyes que protegen las tecnologías de la información y las comunicación, creando problemas y aprovechando los fallos de seguridad .La habilidad del ciberdelincuente le permite realizar estafas, robo de datos personales y comerciales, obteniendo acceso a correos electrónicos, redes sociales, información financiera como, cuentas y claves bancarias.[70]

[67] BANCO SANTANDER.Tipos de ingeniería social.[En Línea].s.f-[19 de noviembre de 2021]-Disponible en:https://www.bancosantander.es/glosario/ingenieria-social
[68] Ibid.
[69] Ibid.
[70] UNIVERSIDAD INTERNACIONAL DE VALENCIA. Ciberdelincuente: Una Nueva Alerta Para Nuestra Seguridad. [En línea].10 de enero de 2022-[21 de octubre de 2022].Disponible en: https://www.universidadviu.com/ec/actualidad/nuestros-expertos/ciberdelincuente-una-nueva-alerta-para-nuestra-seguridad

Figura 2.Vías de ataque ingeniería social.

Fuente: ESYSTEM.Ingeniería Social Tipos de ataques.[imagen].Tecnicas de Ingenieria Social.s.f-[Consultado: 17 de noviembre de 2021].Disponible en: https://www.esystems.com.co/ingenieria-social-que-es/

Se ha podido observar que la forma como se realizan los ataques de ingeniería social es variada y depende de los intereses e imaginación del atacante; en general, los ataques de Ingeniería Social se desarrollan a través de recursos y medios en los cuales se ejecutaran los ataques. Las vías o formas usadas para este fin son:

- ✓ Ataque vía teléfono:
- ✓ Ataque vía Internet
- ✓ *Dumpster Diving o Trashing* (zambullida en la basura).
- ✓ Ataque vía SMS.
- ✓ Ataque cara a cara.

5.1.5 Tipos de ataques: Al escuchar hablar de la ciberdelincuencia, la gran mayoría de usuarios tienen una visión de complejos códigos maliciosos creados para agredir una organización en concreto. Sin embargo, la ciberdelincuencia no actúa siempre de esta manera, ya que ese tipo de ataques exigen una inversión elevada de tiempo y de recursos tanto económicos como humanos, La mayoría de ciberataques busca acechar al mayor número de víctimas, en un tiempo corto y con la mínima inversión. Existen múltiples ataques a la información, que influyen en la Ingeniería Social para conseguirlos, se utilizan ataques desde dos escenarios:

5.1.5.1 Ataques remotos: Los ataques remotos son realizados desde algún protocolo de internet o red, a la distancia, por lo general su objetivo es violentar vulnerabilidades en el sistema, que no podrá lograr sin la intervención de su victimario quien sin saberlo ayudará acceder a estas redes, los ataques remotos generalmente son efectuados a través de:

Redes sociales: Los delincuentes buscan generar una relación cercana con la víctima, de esta manera obtener información gracias a la confianza que se ha generado, ya que las personas tienden a dar a conocer gran parte su vida personal por medio de las redes.
Correos electrónicos el *Phishing*: El atacante envía contenidos con *malware* a sus víctimas, con *links* de páginas clonadas o falsas, haciéndose pasar por organizaciones reales, por ejemplo: (Entidades Bancarias, Establecimientos de comercio, fundaciones, etc.) con la finalidad de robar los datos de accesos ingresadas por las víctimas.
Correos electrónicos *Spear Phishing*: En estos correos electrónicos su objetivo son empleados con perfiles definidos, y con accesos a sistemas informáticos de la organización específicos, en este caso el atacante busca que sea el empleado quien suministre la información interna del cual es responsable.
Técnica Telefónica: El uso del teléfono es una de las técnicas más utilizadas y al parecer más efectivas, ya que es un medio cómodo para el delincuente que mediante una llamada busca manipular las emociones y necesidades de la víctima con una determinada situación, por ejemplo: un problema familiar, la búsqueda de empleo, la gran oferta de un producto, entre otros.
Falsos centros de atención telefónica *(Vishing*): Este ataque remoto se lleva a cabo por servicio telefónico por Internet también conocido como VoIP .De manera que el atacante realiza llamadas haciéndose pasar por un negocio legítimo y así efectuar fraude, de credenciales bancarias.
Teléfonos celulares, el *Smishing* (SMS):El uso de los dispositivos móviles es una técnica común en el que la víctima recibe un mensaje de texto indicando que es ganador de un sorprendente premio, y para reclamarlo debe ingresar a un *link,* devolver la llamada a un número determinado o responder un sms.

5.1.5.2 Ataques Locales. En lo que concierne a los ataques locales, las técnicas utilizadas son:

La técnica *Tailgaiting*: Esta técnica se utiliza cuando hay una restricción de acceso físico en una organización, aquí el delincuente va hacer uso de sus habilidades para decirle a su víctima que no trajo o se le olvido la tarjeta de ingreso, de esta manera manipular a la víctima quien le facilitara el ingreso a la empresa.

La técnica *Pretexting/Impersonate*: En este tipo de ataque, en el que el delincuente dice ser empleado de la misma empresa, manipulando a su víctima por ejemplo, presentándose como funcionario del área técnica, para que este deje

revisar su PC e instalar un *malware* malicioso con el que tendrá ingreso a la información confidencial de este equipo.

Uso de Usbs: Los atacantes hacen uso de usbs con *software* malicioso, mediante la técnica *Baiting,* buscan que la víctima que fue previamente estudiada, conecte este dispositivo que dará el acceso directo a la información que posee.

La técnica *Shoulder Surfing*: Esta técnica se hace por medio de la observación, los delincuentes espían a sus víctimas por encima del hombro, logrando obtener patrones, contraseñas, o códigos que se utilizan en equipos o teléfonos celulares, para poder ingresar en estos dispositivos y escudriñar su información sensible.[71]

5.1.6 Clasificación de técnicas de ingeniería social. Las metodologías utilizadas en este tipo de ataques, también son clasificadas según el nivel de interacción que el delincuente informático tenga con los usuarios. En esta clasificación se encuentran 4 técnicas.

Pasivas: Se basa en la observación; aquí el atacante realiza un análisis del comportamiento del usuario, reconstruyendo su rutina diaria, creando un perfil psicológico, con sus aficiones, hábitos y gustos.
No presenciales: Como su nombre lo indica son llevados a cabo desde la distancia se basan en la solicitud de información mediante correo electrónico o mediante llamadas telefónicas, un ejemplo de esta técnica es el *phishing*.
Presenciales no agresivas: Aquí se le hace seguimiento a la víctima, realizando acciones de vigilancia al domicilio o la búsqueda información en basura, el entorno, mirando encima del hombro, acreditaciones, observación de agendas y teléfonos móviles.
Presenciales agresivas: Como técnicas agresivas se encuentran las presiones psicológicas, la suplantación de identidad, el chantaje y la extorción.[72]

5.1.7 Roles y escenarios de la ingeniería social. En la ingeniería social se asumen uno o varios roles en los diferentes escenarios al momento de realizar un ataque de ingeniería social.

Para ello se crea un escenario inventado donde la víctima se sienta cómoda y suministre su información confidencial.
Esto es mucho más difícil que inventar una simple mentira. En este caso la mentira se convierte en una nueva identidad.

Escenario: Es el lugar donde se ejecutarán las operaciones. Estos escenarios pueden ser lógicos o físicos.

---

[71]BASTO,Marber.Estudio sobre la ingeniería social en las instituciones estatales.[En Línea].Mayo de 2020-[17 de noviembre de 2021].Disponible en:https://repository.unad.edu.co/bitstream/handle/10596/34150/mabastoga.pdf?sequence=1&isAllowed=y
[72] RODRIGUEZ,Ellien.Metodologias de ingeniería social.[En Línea].Junio de 2018-[18 de 2021].Disponible en:http://solutecsos.com/documts/metodologia_ingeniera%20social.pdf

Identidad: Este está ligado al rol; crear una nueva identidad asegura accesibilidad, viabilidad y anonimato en los distintos escenarios que el experimentado ingeniero social se pueda encontrar.

Rol: Tomando un rol se tendrá una identidad con la que se podrá mover en el escenario ya generado, con un rol el atacante lo usará para robar información privilegiada de su víctima. En el área de la ingeniería social es muy empleada para hacerse pasar por un miembro de la organización empresarial «*impersonation*».[73]

La ingeniería social es un conjunto de actividades, metodologías y técnicas, psicológicas y sociales que al ser ejecutadas permiten el acceso a dispositivos informáticos y plataformas, obteniendo como resultado información confidencial y valiosa de los usuarios. Determinar características únicas de un ataque de ingeniería social es muy difícil, pues hay tantas técnicas como tipos de ataques en la actualidad, estos ataques pueden ser efectuados fuera y dentro de la red, de forma presencial o telefónica, por medio de un enlace electrónico, el uso de una USB, un mensaje SMS, una supuesta promoción o premio, aprovechándose de los principios básicos de seres humanos como la confianza, la reciprocidad, la conciencia y la autoridad, utilizando técnicas pasivas, tanto agresivas e involucrando determinado número de interacciones con sus víctimas a fin de lograr su objetivo.

Se podría decir que la principal característica de un ataque de Ingeniería Social es la habilidad social del atacante, ya que este arte social no es desarrollado por todos los seres humanos, La destreza social del ciberdelincuente, mas sus conocimientos en informática, representan una gran amenaza para los usuarios, organizaciones ,entidades financieras y su información.[74]

[73] NAIVENOM.Asumiendo roles en distintos escenarios.[En Línea].s.f-{14 de noviembre de 2021}.Disponible en:https://fwhibbit.es/ingenieria-social-iv-asumiendo-roles-en-distintos-escenarios

[74] MOES;Tibor.¿Que es ingenieria social?5 ejemplos principales.[En linea].s.f-[22 de octubre de 2022].Disponible en: https://softwarelab.org/es/que-es-ingenieria-social/

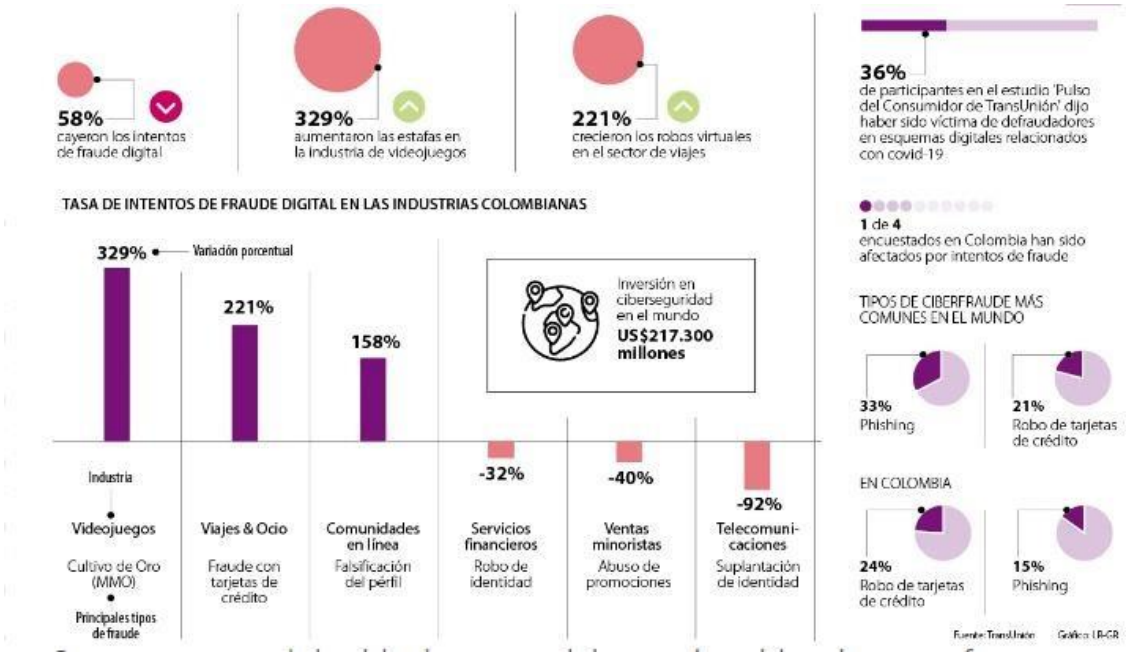
5.2 DESARROLLO OBJETIVO 2: RIESGOS Y AMENAZAS DE LA INGENIERÍA SOCIAL EN SU INTENTO POR QUEBRANTAR LA SEGURIDAD DIGITAL A TRAVÉS DE LA RECOPILACIÓN Y REVISIÓN DE FUENTES DE CONSULTA BIBLIOGRÁFICA, DISPUESTA EN LOS REPOSITORIOS AUTORIZADOS PARA ESTE FIN.

Hoy día es común que distintas industrias realicen sus procesos y trabajen con herramientas cada vez más digitalizadas; La llegada de las cuarentenas y la facilidad de realizar trámites sin salir de casa, incrementó de manera significativa el uso de canales virtuales en múltiples actividades, incluidas las actividades en el sector financiero.

En Colombia para el 2020 la inversión para la lucha contra delitos informáticos y ciberseguridad también incremento en un 20%; obteniendo buenos resultados contra los intentos de fraudes digitales, los cuales cayeron a un 58%.
La Figura a continuación muestra el estudio de Transición donde analizan las tasas de intentos de fraude en las industrias colombianas, en esta se puede observar que han decaído significativamente, los intentos de robo y suplantación de identidad y ha incrementado el fraude en el sector de los video juegos, viajes y ocio con un 329% y 221% respectivamente, así como se destaca intentos de fraude en el abuso de promociones y el robo de tarjetas de crédito. Pese a los esfuerzos y datos alentadores, falta más para radicar de forma definitiva los ataques digitales.[75]

[75] LA REPUBLICA.Los intentos de fraude en el sector financiero cayeron 32% en el segundo trimestre.[En linea].10 de septiembre de 2021-[20 de octubre de 2021].Disponible en: https://www.larepublica.co/finanzas/los-intentos-de-fraude-en-el-sector-financiero-cayeron-32-en-el-segundo-trimestre-3230441

Figura 3. Tasas intentos de fraude en industrias colombianas.



Fuente: Intentos de fraude en el sector financiero. Diario la Republica.[imagen].10 de septiembre de 2021.Disponible en: https://www.larepublica.co/finanzas/los-intentos-de-fraude-en-el-sector-financiero-cayeron-32-en-el-segundo-trimestre-3230441

Riesgo "Es la posibilidad de incurrir en pérdidas por deficiencia, falla o inadecuaciones en, el recurso humano, los procesos, la tecnología, la infraestructura, o por la ocurrencia de acontecimientos externos, que tengan capacidad de incidir en el desarrollo del negocio, para este caso, de la entidad financiera; esta definición incluye el riesgo legal y reputaciones, asociados a tales factores"[76].
Desde el punto de vista de la seguridad de la información existen algunos riesgos relacionados al fraude financiero.

Riesgo de actuación: Es ocasionado cuando por incumplimiento o desconocimiento de las normas y manejo de las tecnologías de la información, se pone en peligro los sistemas informáticos y por ende información sensible.

[76] PATIN, Luis. INGENIERIA SOCIAL: Un ataque a la confianza y al servicio en el sector financiero. [En Línea].Revista digital Vol 7 sept de 2013-[19 de noviembre de 2021].Disponible en:http://apuntesdeinvestigacion.bucaramanga.upb.edu.co/wp-content/uploads/2016/03/6.ESI-Luis-Eduardo-Patin%CC%83o-Dura%CC%81n.pdf

Riesgo Inherente: El riesgo inherente se da con la utilización de la tecnología en los canales electrónicos (audio, cajeros automáticos, Internet, banca móvil, comercios electrónicos, etc.), llevando a cometer errores difíciles de ser controlados, por la naturaleza misma de los servicios.

Riesgo de contagio: Está asociado a la instalación de *software* de origen desconocido mediante el uso de Internet, recepción de *software* o archivos a través de correos electrónicos, lo que los sistemas informáticos se infecten con aplicaciones maliciosas.[77]

5.2.1 Metodología de la Ingeniería Social. No importa el tipo o técnica de ingeniería social que el ciberdelincuente utilice, la metodología siempre es la misma. [78].

Fase de acercamiento
Esta es la primera etapa se busca tener un primer acercamiento con la víctima, para empezar a ganar su confianza, por lo regular el atacante haciendo uso de la ingeniería social permite a la víctima dominar la comunicación porque así detecta sus debilidades primarias a ser explotadas.

Fase de alerta
En esta etapa, su grado de interacción cambia y comienza a ser más activo, refuerza su lazo de confianza, generando cada vez más cuestionamientos; con el objetivo de recibir una gran cantidad de información; replantea la velocidad de sus cuestionamientos; observa el comportamiento que le genera a su víctima estar bajo presión.

Fase de distracción
En esta fase; el atacante ya ha conseguido gran parte de la confianza que necesita para conseguir que su víctima revele información que le interesa. La víctima se siente cómodo en la comunicación y baja sus defensas a niveles penetrables. Mientras tanto, el atacante domina prácticamente la comunicación; siendo muy precavido de no agobiar a su víctima para evitar que éste levante sus alarmas.

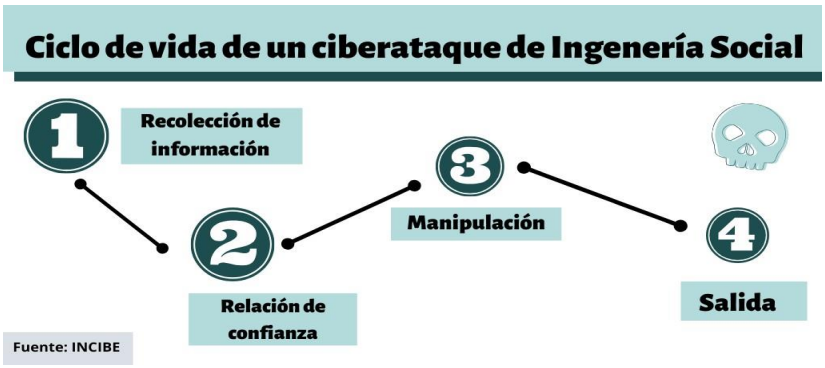
Como parte natural de la interacción y ya completamente envuelto por el atacante; la victima termina entregando información valiosa como, por ejemplo, claves de acceso a cuentas o números de seguridad de sus tarjetas de crédito.

[77] Ibid.,p.3.
[78]ADVISORS. Op. Cit.,

5.2.2 Ciclo de un ataque de ingeniería social. La ciberdelincuencia está en constante movimiento e inventiva, orquestando nuevos modelos de ataques y robos masivos de información, por lo que se hace fundamental estar actualizados y conocer como son ejecutados estos ataques.

Entender el ciclo de vida de un Ciberataque de ingeniería Social, es la primera medida para detectarlos y tomar acciones necesarias que permitan disminuir las posibilidades de sufrir de un ataque de ingeniería social, permitiendo tomar el control de los movimientos y contenidos en la red. Detener cualquier tipo de ataque es posible, en cualquier momento o fase del ataque; Siempre y cuando se reconozcan los pasos y manera de proceder del ciberdelincuente, en el robo de información.[79]

Figura 4.Ciclo de vida de un ataque.



Fuente INTEGRA. El ciclo de vida de un ciberataque de ingenieria social.[imagen].Ingenieria Social. 2020.[consultado: 18 de noviembre de 2021].Disponible en: https://www.productosintegra.com/el-ciclo-de-vida-de-un-ciberataque-basado-en-ingenieria-social/

Un ataque de ingeniería social tiene un ciclo conformado por 4 fases que conforman el ciclo de vida de un Ciberataque de Ingeniería social:

Recolección de la Información. En esta fase el ciberdelincuente recopila la mayor cantidad de información de la víctima objetivo, con el propósito de conocer sus relaciones y datos, entre la información que el atacante quiere obtener están los números de teléfono, Correo electrónico, Dirección de domicilio, Lista de amigos, Lugares frecuentados recurrentemente. [80]:

[79] TORRES,Marcela.Fases de un Ciberataque y como evitarlo.[En Línea].9 de junio de 2022-31 de octubre de 2022].Disponible en: https://creantelab.co/fases-de-un-ciberataque-y-como-evitarlo/

[80] . Cuadernosdeseguridad. [Sitio web]. El ciclo de vida de un ciberataque basado en ingeniería social. Madrid [Consulta: 20 de abril de 2020]. Disponible en: https://cuadernosdeseguridad.com/2020/02/ingenieriasocial-seguridad-incibe/

Desarrollo de la relación: Una vez el atacante ha recolectado la información, tiene ya las herramientas para acercarse a su víctima e iniciar una relación más cercana, entre más confianza más posibilidad de acceder a su información más sensible.

Manipulación: En esta fase el atacante hace uso de la información recolectada y conseguida en los dos pasos anteriores y emplea una manipulación psicológica, logrando tener un acercamiento más a la víctima e indagar y obtener información confidencial aparentemente sin importancia o el acceso concedido y/o transferido al atacante.[81]

Salida: En esta fase el atacante hace su salida por que ya logró cumplir con su objetivo final de ataque, siempre se retira sin levantar sospechas de lo que ha pasado, es tan profesional que no hará cuestionamientos y pondrá fin al ataque antes de que su víctima sospeche lo que está ocurriendo. Además, deja la sensación de haber hecho algo bueno por la víctima, dejando la puerta abierta para futuros acercamientos.

5.2.3 Perfil del atacante. No es fácil reconocer un perfil único del ciberdelincuente, pero existen características generales que se pueden mencionar, como las siguientes:

- ✓ Este puede ser un detective privado, ladrón, espía y hasta podría ser un *hacker.*
- ✓ Siempre actúa en calma y serenidad frente a su víctima.
- ✓ Parece ser el funcionario de alguna organización o entidad financiera.
- ✓ Observa detalladamente a sus víctimas hasta conocer como reaccionaran a sus pretensiones.
- ✓ No expone su integridad, prefiere retirarse si observa que su plan comienza a fallar, Según el desafió es capaz de trabajar en equipo.[82]

5.2.4 Casos de ingeniería social. El acelerado avance tecnológico ha ocasionado desafíos en la mitigación de los nuevos riesgos en la seguridad digital y de acuerdo con Asobancaria,en Colombia el número de denuncias por fraude aumentaron 59%, en el primer semestre de 2020,siendo los relacionados con portal bancario, banca móvil y PSE y banca móvil los más utilizados.[83]

Así han robado cuentas bancarias en el país. El creciente uso de las plataformas digitales ha permitido que múltiples engaños se lleven a cabo en el mundo digital,

[81] Ibid.,
[82] Ibid.,
[83] PORTAFOLIO. Crece el fraude ingeniería social por teléfono.[En Línea]. 27 de septiembre de 2020-[20 de noviembre de 2021].Disponible en:https://www.portafolio.co/economia/crece-fraude-de-ingenieria-social-por-telefono-545060

todo por el desconocimiento o falta de conciencia en las amenazas que son orquestadas en la red.
El periódico el Tiempo indago y documento algunos casos en los que usuarios colombianos han sido víctimas de la ingeniería social, viendo afectadas sus cuentas bancarias, su identidad y hasta su confianza en la tecnología.[84]

El caso del ingeniero Vidal.

> En una tarde cotidiana de trabajo, el ingeniero Ubaldo Vidal tomó su teléfono móvil para hacer una llamada y recibió un mensaje que se convirtió en el inició de una pesadilla que afectó su trabajo, seguridad personal y cuenta bancaria.
>
> En la pantalla de su teléfono se leía 'ni voz ni datos' y aunque inicialmente creyó que se trataba de un error en la red, después descubrió que alguien, a 842 kilómetros de su oficina de Bogotá (en el centro de Montería), se hizo pasar por él para pedirle a su operador de celular el cambio de la SIM *card,* cambiar claves de banco y vaciarle su cuenta.
> "Descubrí la suplantación horas después, luego de pedir un teléfono prestado para marcar a mi número. Al otro lado de la línea un sujeto empezó a reír y a decirme antes de colgar: 'Yo soy Ubaldo'", recuerda Vidal.
>
> Luego de varios minutos de espera, el ingeniero finalmente se comunicó con su operador, Claro, para bloquear la línea –de clase corporativa–, pero allí le informaron que debía presentar un denuncio por pérdida.
>
> Tras dejar constancia de que él tenía en sus manos su SIM *card,* accedió a hacer el trámite, pero ya era tarde. Veinticuatro horas después de que su celular se quedó sin señal, su banco, BBVA, le notificó que se habían aprobado dos jugosas transferencias electrónicas desde su cuenta.
>
> Vidal se convirtió ese día en una de las víctimas de una nueva y sofisticada red de delincuentes que, a través de la reposición de las SIM *card* de los celulares, suplanta a sus dueños y, en cuestión de horas, desocupa cuentas e incluso tramita copia de tarjetas débito y de cédulas para ejecutar delitos mayores.
>
> Y si bien el banco le devolvió el dinero al ingeniero Vidal, él tuvo que vivir una pesadilla de casi dos meses de denuncias, papeleos, presiones y desgaste personal.
> A eso se une la incertidumbre y angustia de saber que alguien tiene acceso a información clave de la vida personal y crediticia.[85]

[84] PORTAFOLIO. Así pueden robar su cuenta bancaria desde celular.[En Línea].Febrero 9 de 2019.[16 de noviembre de 2021].Disponible en:https://www.portafolio.co/economia/finanzas/noticias-hoy-asi-pueden-robar-su-cuenta-bancaria-desde-su-celular-cuenta-de-ahorros-525966
[85] Ibid.

El caso de Catalina Ramírez.

El caso de Ramírez, vinculada a una reputada empresa, incluso prendió las alarmas de la Registraduría, porque los delincuentes alcanzaron a tramitar, vía internet, una contraseña para sacar copia de la cédula de ciudadanía de la joven profesional.

Para la Fiscalía es claro que esta banda accede a datos básicos de sus víctimas antes de ejecutar la suplantación, por eso se indaga la complicidad de empleados que conocen ese tipo de información y que están facilitando el fraude.

En comunicación con el diario, Movistar aseguró que esta modalidad de robo ya le ha generado 20 denuncias en 2018, pero los casos a nivel nacional podrían superar los 2.000.[86.]
La Registraduría acepto que hubo una anomalía al haber aprobado la expedición de una contraseña para sacar el duplicado de la cédula.

"Me enteré de que me estaban suplantando cuando recibí correos de Davivienda, mi banco, notificándome un cambio de contraseña. Alarmada, tramité el bloqueo de mis productos. Luego fui a desbloquearlos, y me indicaron que en el sistema aparecía que un desconocido había recibido una tarjeta débito a mi nombre, a pesar de que la identificación dactilar falló dos veces", dice Ramírez.

La profesional ingresó su número de identidad en la web de la Registraduría y encontró que desde el 8 de noviembre, su cédula estaba en producción de duplicado, luego de que alguien, en Bosa, se hizo pasar por ella.
Luis Fernando Criales, registrador delegado de Registro Civil e Identificación, explicó que la contraseña se puede pedir por internet pagando electrónicamente el trámite. Pero aclaró que el documento final, la cédula, solo se le entrega personalmente al usuario y tras un cotejo biométrico.

"Anualmente, expedimos 4 millones de documentos de identidad, de los que 2,5 millones son cédulas y la mitad de ellas son duplicados. Se puede hacer la trazabilidad del banco y de la IP donde se tramita, pero eso necesita de la previa advertencia del ciudadano que se siente suplantado para enviar la información a las autoridades", precisó Criales.

De hecho, anunció que para el 2019 se habilitará como método complementario el reconocimiento biométrico facial. Además, que se viene realizando la destrucción de documentos (ya van 600.000) que tras un año no son reclamados.

Por ahora, las autoridades rastrean a los jefes de la banda para evitar que sus actividades delictivas tomen mayores dimensiones y que la tecnología se potencie como herramienta a favor del hampa.[87]

[86] Ibid.
[87] Ibid

LA SUPLANTACIÓN UN ATAQUE QUE DE PRODUCE EN SEGUNDOS

La suplantación de identidad a través de plataformas virtuales se puede lograr en 30 segundos; siendo la ingeniería social la técnica más usada por los delincuentes para obtener información personal de sus víctimas; la ingeniería social es una de las formas más eficaces para lograr ese objetivo, este ataque se logra conduciendo a las personas hacia un estado de vulnerabilidad. Utilizando medios como el internet donde envían correos fachada en los que se informa de alguna anomalía en la cuenta bancaria del usuario.

Estos mensajes son aparentemente legales, lo cual hace que las personas sigan las indicaciones que hay en ellos. Cuando esto se da, se descarga secretamente un programa malicioso que les permite a los delincuentes examinar toda la información y movimientos que hace su víctima desde su computador. Sin embargo, la Asociación Bancaria y de Entidades Financieras de Colombia (Asobancaria) ratificó que las transacciones electrónicas son cada vez más seguras.

La Asociación bancaria reconoce que la suplantación de identidad ha migrado de lo presencial a lo virtual, pero hoy en día las sucursales bancarias han implementado sistemas de reconocimiento por biometría y es gracias a este sistema que el número de fraudes se redujo. Notificando así que la transacción electrónica hoy es más segura, ya que solo 3 de cada 100.000 pesos se ven afectados por fraude en internet".

Mientras tanto la Asociación de la Industria Móvil de Colombia (Asomóvil) comunicó que una parte valiosa de estos delitos se realizan a través de celulares robados o de contrabando. Por eso recomiendan a todas las personas adquieran sus dispositivos móviles únicamente en lugares certificados y se evite la manipulación e intervención de terceros.[88]

Suplantando a bancos por llamadas telefónicas buscan robarle su dinero.

El uso del teléfono para realizar fraude bancario es una modalidad de estafa muy común, es utilizada con mayor frecuencia durante la época de Navidad. Suplantando la identidad de entidades bancarias, delincuentes embaucan a los ciudadanos inocentes.
La policía nacional del Centro Cibernético indico que el CAI Virtual recibió más de 20.200 denuncias, entre enero y noviembre del 2019 por estafa realizada en llamada telefónica.

[88] Ibid.

Algunos expertos indican que los delincuentes adquieren ilegalmente bases de datos de diferentes tipos de empresas, y de estas escogen las victimas que van a estafar. Más adelante los atacantes, *hackean* los sistemas informáticos de los bancos y obtienen la información bancaria de los usuarios.
Paso a seguir, una vez obtienen los datos necesarios para perpetrar el delito, haciéndose pasar por funcionarios del banco los delincuentes utilizan diferentes técnicas para 'desocupar' las cuentas de los usuarios bancarios. La modalidad más frecuente es llamar a las víctimas a decirles que sus cuentas reportan movimientos sospechosos y les piden claves y números de tarjetas.

Otra manera, que utilizan es llamar a las personas donde un supuesto asesor comercial realiza una verificación de datos personales mediante la cual el supuesto asesor envía mensaje de texto con códigos de seguridad.
Son tan profesionales en el arte de engañar que la víctima no desconfía y termina por entregar inocentemente todos los datos que los delincuentes necesitan para vaciar sus cuentas".

El Pais.com, documentó la manera en la que los ciberdelincuentes por medio de llamadas telefónicas y haciéndose pasar por funcionarios bancarios, convencen a usuarios de digitar códigos e ingresar a enlaces, que terminan con el robo de cuentas bancarias.[89]

Caso de Claudia Giraldo

> Algo así le pasó a Claudia Giraldo, una enfermera que hace unas semanas fue engañada por un supuesto funcionario del banco donde ella tiene sus cuentas bancarias, para robarle el dinero que ella tenía en estas.
>
> "Me llamaron y me dijeron que necesitaban verificar los datos de una de mis tarjetas porque había una irregularidad, la persona me leyó todos los números de esa tarjeta y me dijo que para hacer la comprobación me iban a enviar a mi celular un mensaje de texto con un código", dijo Claudia
>
> Luego de que los delincuentes generan confianza y logran convencer a las víctimas de que están hablando con un funcionario de la entidad bancaria, así como lo hicieron con Claudia, estos les piden a las víctimas que digiten sus claves, números de tarjetas o códigos de verificación porque con esos datos, logran tener acceso a las cuentas.
>
> "Me pidieron que lo digitara rápido antes de que caducara, ingenuamente yo creí que sí eran del banco y marqué el código, inmediatamente me colgaron y me llegó otro mensaje notificándome de un retiro. Me robaron todo lo que tenía en la cuenta, fueron casi $2 millones", detalló la víctima.

[89]El PAIS.Con llamadas suplantan a bancos.[imagen].Cuidate del phishing.s.f-[Consultado:18 de noviembre de 2021}.Disponible en:https://www.elpais.com.co/judicial/con-llamadas-suplantando-a-bancos-buscan-robarle-su-dinero.html

> Cuando esto sucede, las autoridades manifestaron que es necesario que la víctima recopile todas las evidencias de la estafa y presente el denuncio a través de la plataforma 'A Denunciar' o comunicándose con la Fiscalía mediante la Línea 122.
>
> Asimismo, un funcionario de una entidad bancaria explicó que además de instaurar la denuncia, la persona debe reportar a su banco lo sucedido para que este investigue el caso e igualmente, le colabore con el proceso de cambio de claves y con la devolución del dinero.
>
> Con relación a lo que se debe hacer para no ser víctima de este delito, el funcionario de la entidad financiera indicó que siempre se debe estar alerta porque los estafadores pueden suplantar, incluso, las líneas del banco para que el cliente se sienta confiado.
>
> Además, agregó que "las personas deben tener claro que el banco nunca va a pedir datos confidenciales por llamada, si eres cliente te van a llamar para hablar sobre ofertas del banco o para el tema de cobranza, pero jamás te van a solicitar los números o las claves de las tarjetas".
>
> Finalmente, Raúl Donado comentó que cuando se recibe una llamada de un funcionario de un banco se debe ser precavido. "Una pregunta se debe responder siempre con otra pregunta. Esto permite contrastar información y si es un delincuente, este se impacienta y cuelga, o demuestra que no maneja la situación".[90]

Identificar los riesgos y amenazas consecuencia de ataques de ingeniería social son un factor clave en la prevención y salvaguarda de los sistemas y su información. Reconocer los riesgos brinda la posibilidad de disminuir las fallas o inadecuaciones en la red, en los procesos, la infraestructura, el recurso humano, la tecnología, la infraestructura, o por acontecimientos externos.

La principal amenaza de los sistemas informáticos y la información es el atacante cibernético, este personaje puede aparecer camuflado como un servidor público, o funcionario de entidad financiera, actuara siempre con serenidad y calma, observando muy bien a su posible víctima; quien haciendo uso de su creatividad y de metodologías diseñadas para llevar a cabo su objetivo, buscara un acercamiento con su víctima donde intentara generar el mayor grado de confianza, llegando al punto de tal confianza que su víctima bajara los niveles de defensa por completo, brindando una cantidad de información valiosa. Todos sus ataques llevan una serie de pasos que marcan su accionar; En el caso de la ingeniería social, el primer paso que da el delincuente , es realizar una recolección de información en donde buscara a toda costa encontrar información de números telefónicos, direcciones, correos electrónicos, paso a seguir creara con su víctima un lazo de confianza, una vez generada la confianza, sus interrogatorios serán aún más agresivos para manipular y obtener accesos sin que la otra parte se dé cuenta y por último se retira, muchas veces con la información que se propuso obtener.

[90] Ibid.

Los casos expuestos anteriormente son el reflejo del accionar de la ciberdelincuencia y de la falta de conocimiento y prevención por parte de las personas y las entidades financieras.

5.3 DESARROLLO DE OBJETIVO 3: ESTRATEGIAS Y MÉTODOS DE SEGURIDAD DE LA INFORMACIÓN QUE SE PUEDEN IMPLEMENTAR PARA PROTEGER Y MINIMIZAR LOS RIESGOS OCASIONADOS POR LOS ATAQUES DE INGENIERÍA SOCIAL.

5.3.1 Como Prevenir los ataques de ingeniería social. Contrarrestar un ataque y en especial uno de ingeniería social es una tarea difícil, ya que la responsabilidad tiene un peso especial en el factor humano; Estos ataques creados para sacar provecho de las características humanas como el respeto, la solidaridad, la curiosidad y el respeto por la autoridad; son ataques de ingeniería social aún más complicados de descifrar que complejos códigos maliciosos, sumado a esto el acelerado ritmo del día a día y el creciente uso de los sistemas de información hace al ser humano más vulnerable de ataques de ingeniería social.

Las autoridades, los gobiernos, distintas entidades comerciales y financieras vienen trabajando en una cultura de buenos hábitos en ciberseguridad, donde la concienciación e información son la mejor arma de protección, la figura a continuación es solo una pequeña muestra de las múltiples campañas que se realizan para frenar estos ciberataques.
Seguir los consejos suministrados por las autoridades, estar informado, actualizado, en alerta y siempre a la defensiva, son las acciones aliadas de la seguridad.[91]

[91] WORLDSYS,6 Tips para prevenir ataques de ingeniería social. [En Línea].12 de septiembre de 2022-[30 de octubre de 2022].Disponible en: https://www.worldsys.co/6-tips-para-evitar-un-ataque-de-ingenieria-social/

Figura 5. Prevenir ataques de Ingeniería Social.

Fuente: PINTEREST. No caigas en los ataques de ingenieria social.[imagen]s.f.Disponible en: https://www.pinterest.com.mx/pin/424745808611978987/

La mejor estrategia que existe para proteger a los usuarios de los ataques de ingeniería social es formar y concientizar, de nada sirve contar con un sistema con las medidas de seguridad y tecnologías más modernas, si el personal que lo utiliza no reconoce los peligros existentes y puede ocasionar perdida de la información en un solo clic.

Los ataques de ingeniería social pueden ser variados y realizarse por medio de diferentes técnicas, lamentablemente no hay una fórmula mágica que los evite, por eso son claves en la prevención la concientización y la capacitación en ciberseguridad.

La ingeniería social es una de las técnicas más utilizadas por los atacantes para conseguir sus objetivos delictivos. Para minimizar los riesgos de este tipo de fraude, la mejor vía es formar y concienciar a todas las personas.

Vulnera los principios de la ingeniería social: “Si crees que la tecnología puede solventar tus problemas de seguridad, entonces no entiendes los problemas y no entiendes de tecnología” (Bruce Schneier).[92].

Anteriormente se había hablado de los principios de la ingeniería social y la incidencia de estos en la ejecución de ataques; en esta ocasión se utilizan estos principios a favor de los usuarios, por lo que se les ha llamado vulnerar los principios.

Pertinencia: Hay que ser conscientes que ninguna empresa real solicita números de seguridad social, nombres de usuarios, contraseñas u otros datos similares.
Urgencia: No caer en la mentira de mensajes del tipo “Perderá la información de su cuenta si no responde en un plazo de X horas; este tipo de mensajes buscan desestabilizar al usuario con el fin de que entregue información sensible.
Personalización: La mayoría de las empresas financieras y de comercio, ya saben el nombre de sus usuarios, por eso hay que sospechar de correos electrónicos que no tengan personalización.
Control: Evitar que los impulsos y emociones tomen el control de las acciones. Sentimientos como la intimidación; persuasión; congraciamiento o parecidos serán a los que recurrirán para obtener la información que necesitan. **[93]**

5.3.2 Como evitar estafas telefónicas. Son varios los interrogantes que se generan cuando se oye de ataques que se han realizado por teléfono, interrogantes como: ¿Cómo detectar una estafa telefónica? ¿Qué protección hay que tomar?, son comunes en este caso.
Las estafas vía telefónica no son una práctica nueva en el mundo, pero si es una práctica que está en constante evolución, sortear medidas de seguridad actualmente es más complejo, los delincuentes tienen mucho más dato de sus víctimas, lo que hace más difícil darse cuenta de un engaño.
Actualmente la mayoría de las estafas son realizadas por personas desde la cárcel con ayuda de personas fuera de ellas que son las encargadas de vaciar las cuentas bancarias.
A continuación, alguna de las estafas telefónicas más habituales y cómo reconocerlas.

El Ejecutivo Bancario
Es probable que un día se reciba una llamada de un supuesto agente de banco, con la súper oferta de crédito con precios muy cómodos y una oferta insuperable, que tiene un tiempo ilimitado, pero la condición para activar ese crédito es que se debe consignar cierta cantidad de dinero en una cuenta; Esto es totalmente falso, ninguna entidad pide consignar, ni realizar pagos a cuentas bancarias.

[92]SCHNEIER;Bruce.Las 120 mejores frases sobre la tecnología.Citado por JUÁREZ, Cesar.Psicologia y Mente:febrero 2020
[93]ADVISORS. Op. Cit.,.

Para evitarlo puedes conocer el nombre de tu asesor bancario, identificar los motivos por los que podría, llamar y sobre todo reconocer que por ningún motivo el banco va solicitar datos de contraseñas bancarias o datos similares.

Premio En Concurso

Este tipo de estafa es un clásico, en este caso los estafadores llaman a un número y le dicen a la persona que contesta que ganó un concurso, como por ejemplo el de un carro, pero por supuesto para reclamar el premio debe cumplir con algunas condiciones; llevar dinero a algún lugar, realizar consignación a determinada cuenta, recibir a alguien en su casa y pasarle cosas de valor, ir con tarjetas de crédito o débito a comprar ciertos productos, etc.

Pero la verdad es que ningún tipo de concurso legal pide a cambio una suma de dinero o algún producto.

Para evitar caer en esta estafa es importante vulnerar los principios de la ingeniería social, simplemente no te dejes llevar por la emoción.

El Secuestro

Esta estafa se basa en el principio de la urgencia y la violencia con la que los interlocutores ejecutan el ataque. En la mayoría de los casos, los estafadores conocen información básica de la persona supuestamente secuestrada. Utilizan datos hasta de menores de edad ya que son más difícil contactar, para confirmar lo que está pasando, porque pueden estar en clases. La llamada puede venir de una supuesta mujer llorando, o de niños y personas desesperadas, esto para que la persona se sienta más presionada y acceda a sus pretensiones.

En este engaño la supuesta víctima es incomunicada para evitar que puedan comprobar la veracidad del hecho y extorsionar a la persona contactada.

Recomendaciones para evitar estafas telefónicas.

- ✓ La educación siempre es la mejor arma de prevención, educar a los amigos, familiares y quienes trabajan en la casa; todos deben estar enterados de este tipo de estafas y establecer que antes de entregar cualquier pertenencia a un desconocido se debe contactar primero con los integrantes de la familia.

- ✓ Evitar a toda costa suministrar información personal a desconocidos, desconfíe si están preguntando demás, no comente el número de personas que viven en la casa u horarios en los que está desocupada. Prestar especial atención cuando son los niños que están dando la información, Lo ideal es que no sean ellos quienes contesten el teléfono.

- ✓ No publique su información personal en redes sociales. Es muy fácil concluir hábitos, vacaciones, relaciones sociales y hasta dónde y con quien vive una persona a través de estas plataformas.

- ✓ Se debe mantener la calma en caso de recibir una llamada de urgencia. Lo mejor es colgar y ponerse en contacto con el familiar en cuestión.

- ✓ Los médicos, policías y demás miembros de organizaciones públicas nunca llamaran a pedir dinero, si esto sucede sospeche, puede estar frente a una estafa.

- ✓ Al recibir la llamada de un supuesto funcionario de una entidad bancaria, lo mejor es terminar con la llamada y verificar con el banco la autenticidad de este asesor y la información de las supuestas ofertas que le está ofreciendo.

- ✓ En el caso de recibir una llamada telefónica en el que le indiquen de un supuesto accidente, es conveniente contrarrestar la mentira, por medio de preguntas datos específicos como, el lugar exacto donde ocurrió dicho accidente, que tipo de accidente se tuvo y de donde o qué unidad médica es la que llama o si ya está en el lugar el personal médico y de que hospital o eps vienen.

- ✓ Tener presente que la manera más eficaz de evitar caer en el fraude por teléfono es estar atento y actuar con seguridad y cuidado al momento de recibir alguna llamada sospechosa.

- ✓ Por ningún motivo y nunca los bancos ni otras empresas pedirán información confidencial como claves y contraseñas de acceso por vía telefónica.

- ✓ Una vez más" las claves y contraseñas son personales e intransferibles estas no se comparten con nadie".

- ✓ Desconfié de las llamadas que demuestran cierto grado de urgencia por parte del interlocutor, más cuando este solicita información personal o que adviertan algún riesgo sobre su dinero.

- ✓ Siempre esta alerta al recibir llamadas que prometen, premios, préstamos y ofertas tentadoras.

- ✓ Si sospecha que la llamada que está recibiendo es ilegal, puede argumentar que no cuenta con tiempo o que se encuentra realizando otras actividades, y que tan pronto pueda les devolverá la llamada.

- ✓ Busque información en internet del número desde el que le hicieron la llamada para comprobar si esta línea es legal o si fue reportada por otros usuarios.[94]

5.3.3 Fraudes y estafas *on-line.* Las facilidades y acceso que da internet para realizar compras y transacciones de todo tipo, se ha convertido en blanco de los ciberdelincuentes, quienes ven ahí la oportunidad de estafar y robar datos personales valiosos**.**

Las herramientas y métodos para este tipo de ataques, varían pueden aprovechar las vulnerabilidades presentes en casi todos los programas, o realizar los ataques tradicionales mediante *softwares* malicioso y aplicaciones, hasta creativas estafas de *phishing* diseñadas en cualquier parte del mundo.

Como evitar la estafa *On- Line*

Aprende a reconocer una estafa de *Phishing*: este tipo de ataque conocido como phishing es usado por ciberdelincuentes para estafar a los usuarios con sus cuentas bancarias.

Evita abrir enlaces de sitios *web,* archivos adjuntos de correos electrónicos no solicitados.

No comparta ni revele sus contraseñas a nadie y menos por la red.

Desconfié cuando soliciten mucha información, no proporcione información confidencial en persona, por medio del correo electrónico o por teléfono.

Antes de ingresar a una URL, escríbela en la barra del navegador y no en las páginas de buscadores.

Actualizar continuamente el navegador activando sistemas de seguridad.[95]

5.3.4 Amenazas en dispositivos móviles. El creciente uso de dispositivos móviles y la constante evolución de las aplicaciones, han permitido a las personas realizar actividades de todo tipo, al mismo tiempo que se han convertido en un blanco atractivo para los códigos maliciosos.

Los dispositivos móviles han tenido un notable desarrollo al punto de remplazar un equipo de escritorio, ya que puede realizar casi todas las tareas y operaciones necesarias desde estos dispositivos.

---

[94] BBVA. Cómo protegerse de las estafas telefónicas. [En Línea].10 de septiembre de 2020-[19 de noviembre de 2021].Disponible en:https://www.bbva.com/es/ar/como-detectar-y-protegerse-de-los-ciberdelincuentes-y-las-estafas-telefonicas/

[95]OAS.Estado de la ciberseguridad en el sector Bancario.[En Línea].s.f-[20 de noviembre de 2021].Disponible en :https://www.oas.org/es/sms/cicte/sectorbancariospa.pdfhttps://www.oas.org/es/sms/cicte/sectorbancariospa.pdf

Actualmente, existen muchas aplicaciones con diversas funciones que facilitan tareas que antes eran agotadoras, aplicaciones de bancos, sectores como la salud el comercio y entretenimiento han creado por este medio vínculo con sus usuarios. Toda esa interacción diseñada hoy en día por medio de los dispositivos móviles sin dudarlo trae beneficios, pero no se puede desconocer, los riesgos a los que se está expuesto, por eso a continuación unas recomendaciones para evitar ser blanco de fraude por este medio.

Tener sentido común: Reconocer que existen los peligros y al momento de realizar sus operaciones, apagar su red *wifi* y realizarlo desde los datos de su móvil.

Use antivirus y siempre desconfié: La mejor opción es mantener el dispositivo siempre actualizado; mejor siempre desconfié de las ofertas, ingrese a la página oficial para verificar la información. Al igual a los perfiles oficiales de las empresas.

Evite el secuestro de datos con un *backup*: Con el objetivo de no caer en esta modalidad es valioso tener un respaldo de todos los datos sensibles y críticos del dispositivo móvil. [96]

El hablar de ciberseguridad trae al imaginario que se debe crear protección de forma exclusiva a la tecnología y las redes de datos, dejando de lado al factor humano, primordial en la cadena de seguridad de la información y la comunicación. El atacante o *hacker* se aprovecha de los fallos tecnológicos, así como de las debilidades humanas para actuar, este tipo de ataques se les conoce como

“ingeniería social” y consiste en tender trampas a las personas para que permitan el acceso a redes o datos, divulguen información confidencial, como datos de usuarios y contraseñas.

Este tipo de ataques cuenta con diferentes vías de ataque como lo son los teléfonos, los equipos informáticos, los dispositivos móviles y persona a persona; en los ataques de ingeniería social es muy común que el delincuente haga uso de las debilidades humanas, manifestando urgencia por supuestos accidentes, capturas de familiares, cambios de usuarios y contraseñas por supuestas perdidas de información, la reclamación de premios sorpresa, créditos aprobados, y cuanta publicidad engañosa con la que es fácil vulnerar a las personas y la información que poseen. Algunos consejos para evitar estas modalidades son, siempre indagar la autenticidad de la supuesta oferta o sitio *web*, tomarse el tiempo para pensar, actuar con calma, solicitar datos de información del interlocutor,” de donde llama, cuál es su nombre”, reflexionar y ser realista, los premios y concursos no son fáciles de

[96]EL TIEMPO. Como prevenir estafas por celular.[En Línea].s.f-[19 de noviembre de 2021].Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/prevenir-estafas-por-el-celular-119796

ganar, además de esto proteger los dispositivos con *software* actualizados, ayuda significativamente a la protección de los datos y la información.

Crear una cultura de ciberseguridad, donde la información, la actualización, la capacitación continua y la concienciación frente los ataques de ingeniería social, es la mejor barrera de protección de este tipo de ataques. Pues al reconocer el actuar de la ciberdelincuencia, hace que las personas actúen de forma preventiva y desconfiada, y todos los tramites e información que circula en bases de datos, redes sociales, sean verificados siempre antes de tomar una decisión y *cliclear* o suministrar información donde no se debe y a quien no se debe.[97]

¡La desconfianza es el mejor aliado de la seguridad!

[97] KASPERSKY.Maneras de evitar ataques de ingenieria social.[en línea].s.f-[29 de octubre de 2022].Disponible en:https://www.kaspersky.es/resource-center/threats/how-to-avoid-social-engineering-attacks

6 CONCLUSIONES

En base al desarrollo de los objetivos específicos planteados en esta monografía se puede concluir que:

Existen diversas formas de llevar a cabo ataques de ingeniería social y las características de estos ataques son tan variados como los mismos ataques; todos con el propósito de vulnerar la seguridad de la información almacenada en el que es considerado el eslabón más débil dentro de la cadena de seguridad de la información, “el ser humano”; quien posee información sensible y a quien puede ser muy fácil de persuadir y atacar por medio de los principios básicos de la ingeniería social y a los distintos canales o mejor dicho, vías de ataque en los que se pueden efectuar este tipo de ataques, cómo lo es de forma personal, por medios electrónicos, vía telefonica,enlaces,campañas falsas, *apps* malisiosas,Ataques vía SMS entre otros.

El atacante aprovechará al máximo la ingenuidad y desconocimiento de las personas acerca de la ingeniería social, que generará la confianza suficiente para obtener información de manera tan fácil y sin que la víctima se dé cuenta de lo que está sucediendo.

Por medio de la recopilación y posterior revisión de fuentes de consulta encontrados en repositorios académicos y en la web, se deduce que los riesgos y amenazas de sufrir un ataque de ingeniería social se encuentran latentes en todos los aspectos y escenarios del actual vivir, la virtualidad trae consigo amenazas que suponen un manejo de información sensible e importante; Los ataques de ingeniería social se logran llevar a cabo debido a que el delincuente examina muy bien a su víctima, recopila la mayor información posible ,para así acercarse a su víctima, ganarse su confianza hasta lograr este baje por completo sus defensas y lograr su objetivo, la obtención de información muy valiosa como números y movimientos de cuentas bancarias, claves de acceso, números de seguridad de tarjetas.

La estrategia más eficaz existente para proteger la información de las personas de los ataques de ingeniería social es educar y concientizar, poco o nada sirve contar con medidas de seguridad, sistemas y tecnologías modernas, si el personal que hace uso de estas no identifica las amenazas existentes. Los ataques de ingeniería social son tan variados y pueden realizarse por medio de distintas técnicas; no existe una estrategia única que evite ser blanco de la ingeniería social, por eso es clave la prevención, la concientización y la capacitación de todas las personas en temas de ciberseguridad, para minimizar los riesgos y amenazas de este tipo de fraude.

7 RECOMENDACIONES

En el desarrollo de la presente monografía, se analiza y determina las características de las técnicas de ingeniería social que son utilizadas para atacar a usuarios de entidades financieras, se determinan las principales características de estos ataques y los esfuerzos y estrategias de las entidades financieras por frenar estas amenazas.

Todos estos esfuerzos con el objetivo de garantizar que la información que cada una de las personas deposita en los sistemas informáticos sea salvaguardada; Aún falta mucho por hacer al respecto por tal motivo, una vez concluido el presente trabajo monográfico se pone a disposición de los lectores las siguientes recomendaciones:

Para futuros trabajos se recomienda realizar una propuesta de capacitación con herramientas virtuales al personal tanto interno como externo de entidades financieras que abarque las estrategias que se pueden implementar a fin de evitar ataques producto de la ingeniería social y consolidar una cultura de protección de la información.

Asimismo, se recomienda al sector financiero diversificar y aumentar sus políticas de seguridad informática conjuntamente con las autoridades públicas, con el propósito de educar a los usuarios acerca de las precauciones a tener en la utilización de los diferentes servicios financieros disponibles en la red, disminuyendo con esto la probabilidad de ser blanco de los delincuentes informáticos.

A cada uno de los lectores de esta monografía se les sugiere ampliar información acerca de métodos de seguridad de la información tales como; configuración de filtros *spam* de un alto nivel, protección de dispositivos informáticos, antivirus,cortafuegos,*firewalls,* aplicaciones de encriptación, ciberseguridad biométrica,etc,todos estos con el propósito de robustecer los niveles de seguridad de la información; pero sobretodo se aconseja no confiar en que este tipo de métodos de seguridad por si solos libraran de un ataque de ingeniería social;, si bien los métodos descritos anteriormente aumentan en gran medida la capacidad de protección de los sistemas de información es importante mantener los *software* actualizados y sobre todo desconfiar y verificar la autenticidad de supuestos interlocutores, enlaces, páginas, promociones; el tesoro de la información también es responsabilidad propia.

BIBLIOGRAFÍA

ADVISORS. Riesgos y amenazas de la ingeniería social.{En Línea}.27 de febrero de 2018-{18 de noviembre de 2021}.Disponible en: https://www.gb-advisors.com/es/riesgos-y-amenazas-de-la- ingenieria-social/

AETECNO. Banca y salud los principales blancos de ataques. {En Línea}.6 de marzo de 2020-{17 de septiembre de 2021}.Disponible en: https://tecno.americaeconomia.com/articulos/banca-salud-e- ingenieria-social-son-los-principales-blancos-de-los-ciberataques-en

ALCALDIA DE BOGOTA.Ley 1341 de 2009.{En Línea}.s.f-{17 de nov de 2021}.Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913BANCO

SANTANDER. Tipos de ingeniería social.{En Línea}.s.f-{19 de noviembre de 2021}-Disponible en: https://www.bancosantander.es/glosario/ingenieria-social

BASTO, Marber. Estudio sobre la ingeniería social en las instituciones estatales.{En Línea}.Mayo de2020-{17 de noviembre de 2021}.Disponible en: https://repository.unad.edu.co/bitstream/handle/10596/34150/mabastoga.pdf?sequence=1&isAll owed=y

BBVA. Cómo protegerse de las estafas telefónicas.{En Línea}.10 de septiembre de 2020-{19 de noviembre de 2021}.Disponible en:https://www.bbva.com/es/ar/como-detectar-y-protegerse-de-los- ciberdelincuentes-y-las-estafas-telefonicas/

BELCIC, Iván. ¿Qué es inyección SOL?{En Línea}.22 de septiembre de 2020-{3 de octubre de2021}.Disponible en: https://www.avast.com/es-es/c-sql-injection

BERENGER, David. Estudio de Metodologías de Ingeniería Social.{En Línea}.Junio de 2018-{10 de noviembre de 2021}.Disponible en:http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

BID. Mensajes Institucionales.{En Línea}.Julio de 2020-{6 de septiembre de 2021}.Disponible en:Reporte Ciberseguridad 2020: riesgos, avances y el camino a seguir en América Latina y el Caribe| Publications (iadb.org)

BODNAR,Danielle.¿Que es Ingeniería Social Y cómo evitarla?.{En Línea}.29 de octubre de 2020-{15 de octubre de 2021}.Disponible en: https://www.avast.com/es-es/c-social-engineering

CISCO. ¿Qué es Ciberseguridad?.{En Línea}.s.f-{20 de septiembre de 2021}.Disponible en:https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL. Política general de seguridad Nacional. {En Línea}.11 de abril de 2016-{22 de septiembre de 2021}.Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

CORDERO, William. IMPLEMENTACION DE TECNICAS DE INGENIERIA SOCIAL EN LA INSTITUCION EDUCATIVA TECNICA DE PANQUEBA.{En Línea}.2018-{12 de octubre de 2021}.Disponible en:https://repository.unad.edu.co/bitstream/handle/10596/22690/91532860.pdf?sequence=1&isAllo wed=y

CUADERNOS DE SEGURIDAD... El ciclo de vida de un ciberataque basado en ingeniería social. [Sitio web] Madrid [Consulta: 20 de abril de 2020]. Disponible en: https://cuadernosdeseguridad.com/2020/02/ingenieriasocial-seguridad-incibe/

DEPARTAMENTO DE LA FUNCION PÚBLICA. Ley estatutaria 1581 de 2012.{En Línea}.s.f-{18 denoviembre de 2021}.Disponibleen:https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

DEPARTAMENTO DE LA FUNCIONPUBLICA. LEY 1328 DE 2009.{En Línea}.s.f-{20 de nov de 2021}.Disponible en: https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=36841

El PAIS. Con llamadas suplantan a bancos.{En Línea}.s.f-{18 de noviembre de 2021}.Disponibleen. https://www.elpais.com.co/judicial/con-llamadas-suplantando-a-bancos-buscan-robarle-su- dinero.html

EL TIEMPO. Como prevenir estafas por celular.{En Línea}.s.f-{19 de noviembre de 2021}.Disponible en: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/prevenir-estafas-por-el-celular-119796

ESYSTEM. Ingeniería social.{En Línea}.s.f-{15 de octubre de 2021}.Disponible en: https://www.esystems.com.co/ingenieria-social-que-es/

GBADVIRSORS. Riesgos y Amenazas de la Ingeniería Social.{En Línea}.27 de febrero de 2018-{14 de septiembre de 2021}.Disponible en: https://www.gb-advisors.com/es/riesgos-y-amenazas-de-la- ingenieria-social/

GDATA. Que es realmente la ingeniería social.{En Línea}.s.f-{15 de noviembre de 2021}.Disponible en: https://www.gdata.es/guidebook/what-actually-is-social-engineering

GERENCIE. COM. Que es táctica.{En Línea}.27 de noviembre de 2020-{8 de octubre de 2021}.Disponible en: https://www.gerencie.com/diferencia-entre-tactica-y-estrategia.html

HERNANDEZ, Camilo. ¿Qué tipos de ciberataques existen?{En Línea}.9 de julio de 2020-{1 de octubre de 2021}.Disponible en: https://incp.org.co/que-tipos-de-ciberataques-existen/=y

IGLESIAS, Pablo. Los Principios Básicos De La Ingeniería Social.{En Línea}.s.f-{16 de noviembre de 2021}.Disponible en: https://www.pabloyglesias.com/mundohacker-ingenieria-social/

INFOSECURITY. Ciberseguridad.{En Línea}.s.f-{5 de octubre de 2021}.Disponible en: https://www.infosecuritymexico.com/es/ciberseguridad.html

ISO, Tools. ¿Que significa Seguridad Informática?{En Línea}.21 mayo de 2015-{10 de 0ctubre de 2021}.Disponible en: https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/

LATAM, Kaspersky. ¿Qué es Ciberseguridad?.{En Línea}.s.f.-{5 de octubre de 2021} https://latam.kaspersky.com/resource-center/definitions/what-is-cyber-security

LEDESMA, Cristina. Ingenieria social.{En Línea}.s.f-{8 de septiembre de 2021}.Disponible en: https://www.magazcitum.com.mx/index.php/archivos/2747#.YZkQuWDMKM8

LISA, Institute. Guia Practica Ingeniería Social.{En Línea}.8 de mayo de 2020-{17 de septiembre de 2021}.Disponible en: https://www.lisainstitute.com/blogs/blog/guia-practica-ingenieria-social

MENDEZ, Alejandro. Estudio de Metodologías de Ingeniería Social.{En Línea}.Diciembre de 2018-{12de noviembre de 2021}.Disponible en : http://openaccess.uoc.edu/webapps/o2/bitstream/10609/90305/6/amendezcarTFM12189memoria.pdf

NAIVENOM. Asumiendo roles en distintos escenarios.{En Línea}.s.f-{14 de noviembre de 2021}.Disponible en: https://fwhibbit.es/ingenieria-social-iv-asumiendo-roles-en-distintos-escenarios

NORTON. Que es la ingeniería social.{En Línea}.s.f-{6 de septiembre de 2021}.Disponible en: https://co.norton.com/internetsecurity-emerging-threats-what-is-social-engineering.html

OAS. Estado de la ciberseguridad en el sector Bancario.{En Línea}.s.f-{20 de

noviembre de2021}.Disponible en:
https://www.oas.org/es/sms/cicte/sectorbancariospa.pdfhttps://www.oas.org/es/sms/cicte/sectorban cariospa.pdf

OXFORD, Languages. Definición de Ciberseguridad. {En Línea}. s.f- {20
De septiembre de2021}. Disponible en: https://languages.oup.com/google-dictionary-es/

PATIN, Luis. INGENIERIA SOCIAL: Un ataque a la confianza y al servicio en el sector financiero.{EnLínea}.s.f-{19de noviembre de 2021}.Disponible en: http://apuntesdeinvestigacion.bucaramanga.upb.edu.co/wp-content/uploads/2016/03/6.ESI-Luis-Eduardo-Patin%CC%83o-Dura%CC%81n.pdf

PICHINCHA. Ataques de Ingeniería Social.{En Línea}.s.f-{12 de septiembre de 2021}.Disponible en: https://www.pichincha.com/portal/blog/post/ataques-ingenieria-social

PLAZAS, Edna. Ingeniería social en las empresas colombianas. {En Línea}.2018-{18 de septiembrede 2021}.Disponible en:
https://repository.unad.edu.co/bitstream/handle/10596/18704/1094921881.pdf?sequence=1&isAl lowed=y

PORTAFOLIO. Así pueden robar su cuenta bancaria desde celular.{En Línea}.Febrero 9 de 2019.{16 de noviembre de 2021}.Disponible en: https://www.portafolio.co/economia/finanzas/noticias-hoy-asi- pueden-robar-su-cuenta-bancaria-desde-su-celular-cuenta-de-ahorros-525966

PORTAFOLIO. Crece el fraude ingeniería social por teléfono.{En Línea}. 27 de septiembre de 2020-{20 de noviembre de 2021}.Disponible en:
https://www.portafolio.co/economia/crece-fraude-de-ingenieria-social-por-telefono-545060

RAMÍREZ, Jorge; Ingeniería Social, una amenazainformática
http://es.scribd.com/doc/19394749/Ingenieria-social-una-amenaza-informatica

RODRIGUEZ, Ellien. Metodologías de ingeniería social.{En Línea}.Junio de 2018-{18 de 2021}.Disponible en:
http://solutecsos.com/documts/metodologia_ingeniera%20social.pdf

SANDOVAL, Edgar. Ingeniería Social: Corrompiendo la mente Humana.{En Línea}.s.f-{10 de septiembre de 2021}.Disponible en: https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana

SECRETARIA DEL SENADO. Ley 1273.{En Línea}.20 oct de 2021-{17 de noviembre de2021}.Disponible en:
http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

SECRETARIA DEL SENADO.{En Línea}.Ley 1266 de 2008-{13 de noviembre de 2021}.Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1266_2008.html

SIGNIFICADOs.COM. “Técnica”.{En Línea}.s.f-{17 de octubre de 2021}. Disponible en: https://www.significados.com/tecnica/

UNIR.QUE ES LA SEGURIDAD DE LA INFORMACION. {En Línea}.15 de junio de 2021-{8 de octubre 2021}.Disponible en: https://ecuador.unir.net/actualidad-unir/que-es-seguridad-informatica/