# INGENIERÍA SOCIAL A TRAVÉS DE CORREOS ELECTRÓNICOS Y REDES SOCIALES EN EMPRESAS DEL SECTOR FINANCIERO Y ENTIDADES GUBERNAMENTALES COLOMBIANAS ENTRE LOS AÑOS 2015 Y 2020

LUIS ALBERTO ORTIZ PALMA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
POPAYÁN
2021

# INGENIERÍA SOCIAL A TRAVÉS DE CORREOS ELECTRÓNICOS Y REDES SOCIALES EN EMPRESAS DEL SECTOR FINANCIERO Y ENTIDADES GUBERNAMENTALES COLOMBIANAS ENTRE LOS AÑOS 2015 Y 2020

LUIS ALBERTO ORTIZ PALMA

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

Yolima Esther Mercado Palencia
Directora/Asesora

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
POPAYÁN
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Popayán., diciembre 23 de 2021

## DEDICATORIA

Dedico este proyecto a todas las personas que han contribuido en mi formación a lo largo de vida. En primer lugar, a mi familia por todo el apoyo y motivación durante este proceso de formación profesional. En segundo lugar, a mi novia por todo el apoyo y la motivación constante para que concluyera este trabajo. También se la dedico a los buenos amigos y demás personas que han apoyado incondicionalmente.

## AGRADECIMIENTOS

A todos quienes han contribuido al proceso y conclusión de este trabajo, a la Universidad Nacional Abierta y a Distancia UNAD, lugar de crecimiento académico y profesional, también al Departamento de Ingeniería de Sistemas y a los verdaderos tutores, aquellos que tienen la vocación de enseñar, que construyen y buscan la forma para sacar adelante a sus estudiantes. A todos por sus aportes y recomendaciones.

Es un momento muy especial que espero, prevalezca en el tiempo, no solo en la mente de las personas a quienes agradecí, sino también a quienes invirtieron su tiempo para leer esta monografía, a todos les agradezco con todo mi ser.

**CONTENIDO**

pág.

## LISTA DE TABLAS

pág.

## LISTA DE FIGURAS

pág.

## LISTA DE GRÁFICOS

pág.

## GLOSARIO

AMENAZA: Posibilidad de que ocurra un evento que genere daños a un activo o sistema informático y atente contra la seguridad informática.

*BAITING*: Ataque de ingeniería social que usa un gancho para atraer la victima mostrando algo tentador bien sea una gran oferta, algo gratis o una cosa novedosa o de último momento y de esta forma tenderle una trampa y robarle información sensible.

CONTROLES DE SEGURIDAD: Mecanismos utilizados para garantizar la confidencialidad, disponibilidad e integridad por medio del control de accesos y privilegios.

CORREO ELECTRÓNICO: Medio digital a través del cual las personas apoyadas en un dispositivo electrónico y la red informática pueden enviar y recibir archivos, documentos o mensajes.

ESTANDAR DE CIBERSEGURIDAD: Es un conjunto de normas y políticas creadas por una organización reconocida y que busca estandarizar, optimizar, proteger y garantizar la seguridad de las herramientas tecnológicas que usan las personas u organizaciones.

*FARMING*: Consiste en establecer comunicaciones previas con la víctima con el fin de recopilar la mayor información posible para luego abordar a la víctima por correo electrónico e intimidarla bajo amenazas con publicar supuesta información intima o en realizar futuros ataques a la empresa donde este trabaja.

INFORMACIÓN: Conjunto de datos con significado y que están disponibles para estructuración, análisis y toma de decisiones.

INGENIERÍA SOCIAL: Es una modalidad de robo de información sensible y privada de las victimas utilizando la manipulación, el engaño y llegando a estos por medio del establecimiento de estrategias que generen lazos de confianza o la ingenuidad de las personas.

*MALWARE*: Programa dañino que se infiltra y afecta a los sistemas informáticos y equipos electrónicos y que es conocido por realizar acciones sin consentimiento del usuario.

NIST: Estándar internacional NIST (Instituto nacional de estándares y tecnología) del departamento de comercio de los Estados Unidos dedicado a la promoción de competencia industrial y la innovación por medio del trabajo constante en la estandarización de la metrología normas y tecnología.

POLITICAS DE SEGURIDAD: Conjunto de normas y directivas que buscan garantizar la confidencialidad, disponibilidad e integridad y mitigar el impacto de los riesgos.

*PHISHING*: Técnica de suplantación de identidad (persona, empresa) para conseguir información sensible a partir del engaño, la manipulación y el abuso de confianza de la víctima.

RED SOCIAL: Conjunto de individuos que interactúan debido a que comparten ciertos lazos, características y/o afinidades comunes.

RIESGO: Probabilidad que ocurra un incidente de seguridad y genere perdidas o daños por la materialización de una amenaza

SEGURIDAD INFORMÁTICA: Es la encargada de realizar la protección del sistema informático a través de un conjunto de soluciones técnicas que centran su esfuerzo en la infraestructura y comunicaciones (TIC) para garantizar la integridad y confidencialidad la

información que contienen. Se trabaja con las vulnerabilidades y con amenazas en forma de ataques.

SEGURIDAD DE LA INFORMACIÓN: Es la encargada de regular y establecer las pautas a seguir para la protección de la información en todos los medios donde se localice la información independientemente del estado en que se encuentre. Para la aplicación y gestión de las medidas de seguridad para lo cual se apoya en la seguridad informática y además se hace uso de metodologías, normas, técnicas, herramientas, estructuras organizacionales, tecnología entre otros. Para garantizar la integridad, disponibilidad y confidencialidad de la información se trabaja en un sistema de gestión de la seguridad de la información a nivel de vulnerabilidades, amenazas y riesgos.

VULNERABILIDAD: Condiciones que permiten a un sistema informático ser susceptible de sufrir un daño y afectar negativamente la seguridad de la información frente a una amenaza.

## RESUMEN

Avanza la tecnología y también lo hacen los delincuentes informáticos. La ingeniería social es la técnica más antigua y que hoy es de gran efectividad pues permite vulnerar cualquier sistema por más robusto que sea, aplicando el engaño en las personas. De allí la importancia de conocer el desempeño de los sistemas de gestión de la seguridad de la información y los riesgos a los que se enfrenta la información de una organización.

Esta monografía compila y hace un análisis sobre casos de ingeniería social reportados en Colombia a partir de la información bibliográfica y los resultados de investigaciones realizadas al interior de diferentes empresas del sector financiero y entidades gubernamentales colombianas entre los años 2015 y 2020 evidenciando las técnicas y estrategias de ingeniería social más utilizadas como son *phishing* en correos electrónicos y la recopilación de información a través redes sociales y el *baiting*. Actualmente, la mayoría de las empresas han migrado a plataformas electrónicas usando redes sociales y correo electrónico para interactuar con sus clientes de forma efectiva y rápida, sin embargo, esto atrajo la atención de atacantes informáticos quienes buscan información de incautos y realizan extorsiones. Esto implica un peligro para la integridad, confidencialidad y disponibilidad de la información en empresas y personas. Esta monografía busca generar conciencia en las personas por medio de la visualización y análisis de casos y técnicas de extorsión más utilizadas por parte de los delincuentes informáticos a nivel de ingeniería social.



PALABRAS CLAVE: Ingeniería social, correos electrónicos, Redes sociales, Seguridad, Información, Colombia.

## ABSTRACT

Technology advances and so do computer criminals. Social engineering is the oldest technique, and today it is highly effective because it allows any system to be breached, no matter how robust it may be, by deceiving people. Hence the importance of knowing the performance of information security management systems and the risks faced by an organization's information.

This monograph compiles and analyzes cases of social engineering reported in Colombia based on bibliographic information and the results of research conducted within different companies in the financial sector and Colombian government entities between 2015 and 2020, showing the most commonly used social engineering techniques and strategies such as *phishing* in emails and information gathering through social networks and *baiting*. Currently, most companies have migrated to electronic platforms using social networks and email to interact with their customers effectively and quickly, however, this attracted the attention of computer attackers who seek information from unsuspecting and perform extortion. This implies a danger to the integrity, confidentiality and availability of information in companies and individuals. This monograph seeks to raise awareness in people through the visualization and analysis of cases and extortion techniques most commonly used by computer criminals at the social engineering level.



KEY WORDS: Social engineering, e-mails, Social networks, Security, Information, Colombia.

# INTRODUCCIÓN

El uso de ingeniería social para engañar a personas continúa vigente y es una de las técnicas comunes que utilizan los delincuentes informáticos para acceder a información confidencial. Hoy en día, recurrir a vulnerar la confianza de las personas resulta más fácil que atacar los algoritmos y plataformas de una empresa. Entre los medios utilizados para hacer ingeniería social se encuentran los correos electrónicos y redes sociales, canales electrónicos que cada día son más utilizados y que tienen mayor crecimiento debido a la ampliación de la cobertura de las redes de datos y la accesibilidad multiplataforma a contenidos digitales a través de dispositivos móviles, tabletas y prácticamente con cualquier dispositivo conectado a internet.

Pero tal como surgen nuevas formas de acceder a la información, también aparecen nuevas amenazas, por ejemplo, el uso de *phishing*, una técnica de ingeniería social que aprovecha personas incautas, con pocos conocimientos en sistemas de información y empresas que no cuentan con planes de seguridad informática bien estructurados que garanticen una correcta socialización y capacitación a sus trabajadores en temas de ingeniería social[1]. Es así como para combatir ataques de ingeniería social los expertos en seguridad informática y los diferentes modelos y estándares del Sistema de Gestión de la Seguridad de la Información (SGSI) han coincidido en que aparte de la seguridad de los sistemas informáticos es necesario trabajar en la capacitación periódica a empleados y personal de una empresa. Es necesario socializar información precisa y actualizada sobre los diferentes tipos de ataques y técnicas utilizadas por los ciberdelincuentes y empoderar a la persona para que esté alerta y sepa cómo enfrentar una situación encaminada a ataques de ingeniería social.

[1] GOBIERNO DE ESPAÑA, INCIBE. *Phishing* [sitio web]. Madrid; [Consultado: 07 de mayo de 2021]. Disponible en: https://www.incibe.es/aprendeciberseguridad/phishing

En Colombia el uso de ingeniería social representa un gran porcentaje de los ataques a empresas. De acuerdo con el informe del 2019 sobre Cibercrimen en Colombia de la Policía Nacional Colombiana hay 17531 casos de ataques informáticos, notándose un incremento respecto al 2018 del 54%, donde los mayores casos se generaron en Bogotá (5308), Cali (1190), Medellín (1186), Barranquilla (643) y Bucaramanga (397) donde los principales delitos son hurto de medios electrónicos para robo de dinero con 31058 casos reportados; Violación de datos personales con 8037 casos, donde el objetivo es el robo de identidad para empresas y personas; acceso abusivo al sistema informático con 7994 casos, donde buscan comprometer sistemas informáticos a través del acceso por ingeniería social; transferencia no consentida de activos con 3425 casos, encaminada a extraer dinero o transferir activos financieros de las víctimas; finalmente se encuentra el uso de *software* malicioso con 2387 casos[2] .

El presente documento contiene la compilación de las técnicas y metodologías de ingeniería social y el análisis del impacto de los ciberataques realizados a través de correos electrónicos y redes sociales en empresas del sector financiero y entidades gubernamentales colombianas entre los años 2015 y 2020. Además, se muestra una clasificación de las principales vulnerabilidades y amenazas utilizadas para realizar ataques de ingeniería social y algunas recomendaciones.

[2] POLICIA NACIONAL DE COLOMBIA [sitio web]. Bogotá. CAI VIRTUAL. Tendencias Cibercrimen en Colombia. [Consultado: 20 de septiembre de 2020]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

# 1. DEFINICIÓN DEL PROBLEMA

## 1.1 ANTECEDENTES DEL PROBLEMA

El uso de ingeniería social para engañar a personas continúa vigente y es una de las técnicas comunes que utilizan los delincuentes informáticos para acceder a información confidencial. Hoy en día, recurrir a vulnerar la confianza de las personas resulta más fácil que atacar los algoritmos y plataformas de una empresa. Entre los medios utilizados para hacer ingeniería social se encuentran los correos electrónicos y redes sociales, canales electrónicos que cada día son más utilizados y que tienen mayor crecimiento debido a la ampliación de la cobertura de las redes de datos y la accesibilidad multiplataforma a contenidos digitales a través de dispositivos móviles, tabletas y prácticamente con cualquier dispositivo conectado a internet.

Existen algunas investigaciones y trabajos de campo que buscan conocer cual la posibilidad de materializar ataques de Ingeniería social en Instituciones educativas de educación superior entre los que se encuentra el de Acosta, en el 2018 quien muestra que para las instituciones de educación superior la técnica más utilizada es la suplantación de identidad por medio de *phishing* la cual tiene éxito debido a que los atacantes aprovechan el desconocimiento de ciertas personas y que muchas universidades tienen una unidad o dependencia encargada de la gestión de los servicios tecnológicos, sin embargo, su orientación está hacia la seguridad se basa únicamente en la seguridad del componente físico y lógico[3].

Es importante tener en cuenta el tema de seguridad informática desde los ataques provenientes de ingeniería social ya que si bien es cierto la implementación de sistemas

[3] ACOSTA PINEDA, Santiago *et al*. Ingeniería social en instituciones de educación superior. En: Tecnologías de avanzada [en línea]. Norte de Santander: Revista Colombiana de Tecnologías de Avanzada UNIPAMPLONA, abril-junio de 2018, vol., 2, nro. 32. 10 p. [Consultado: 23 de septiembre de 2020]. Disponible en http://revistas.unipamplona.edu.co/ojs_viceinves/index.php/RCTA/article/view/2370/0. ISSN 1692-7257.

como *firewalls*, antivirus y canales seguros para el envío de información son muy importantes para robustecer un sistema, poco pueden hacer si no se controla el comportamiento de las personas frente al uso que le den a las diferentes herramientas informáticas de la empresa. Sumando a la ingenuidad o desconocimiento de las personas en las empresas se encuentra la negativa de los gerentes, presumen saber del tema y lo ven como algo impalpable y muy elemental, no creen que haya ingenuidad entre sus trabajadores, pues son profesionales capacitados, así que es un gasto innecesario, además demanda tiempo para capacitaciones, lo cual es tiempo improductivo para sus empresas. Solamente se hacen las respectivas reflexiones cuando su información fue atacada o hubo extorsiones y se cuestionan sobre la importancia de haberlo realizado antes.

Lo anterior se puede contrastar con lo encontrado por Castellanos, 2019 en una prueba piloto realizada a un grupo de estudiantes del programa de ingeniería de sistemas de la universidad católica de Colombia, donde se encuentra que al realizarles una encuesta antes de la prueba todos presumen saber del tema y jamás van a ser engañados porque saben de seguridad informática pero al realizarles un ataque controlado de ingeniería social por medio de *phishing* la mayoría fueron víctimas y cayeron en el engaño[4].

El éxito de las técnicas de ataques por medio de *phishing* se deben a la falta de conocimiento y ausencia de políticas definidas de gestión de seguridad es así como por ejemplo en la ciudad de Neiva se detectó falencias en los sistemas de TI de la Universidad Cooperativa de Colombia y según su autor la institución es vulnerable de ataques de ingeniería social, ya que se encontraron deficiencias en capacitación sobre seguridad informática y de la información y desconocimiento por parte de los trabajadores. Entendiéndose la seguridad informática como aquella encargada de brindar la seguridad

[4] CARVAJAL, Hernán Darío y CASTELLANOS, John. Ataque controlado de ingeniería social usando códigos QR [en línea]. Trabajo de grado especialización en seguridad de la información. Bogotá. Universidad Católica de Colombia. Facultad de ingeniería. Departamento de Sistemas, 2019. 98 p. [Consultado: 12 de noviembre de 2020]. Disponible en: Repositorio Educativo Digital UCATOLICA. https://repository.ucatolica.edu.co/jspui/handle/10983/24063

de la información desde la infraestructura y la seguridad de la información que aporta con la definición de políticas, normas y buenas prácticas para proteger la información[5]. Lo anterior en conjunto crea las mejores prácticas y permite cumplir con los principios de la triada de la seguridad (confidencialidad, disponibilidad, integridad).

Además de lo anterior, existen falencias en la asignación de claves de usuario robustas en equipos de cómputo y ausencia en control de puertas de acceso, ni registro y control de personas. Es relativamente fácil realizar un ataque de Ingeniería Social a través de alguna de sus técnicas, por ejemplo, suplantación de identidad a través de llamadas telefónicas, la de espiar por encima del hombro, la de desarrollar confianza, la sobrecarga, la de escuchar detrás de las puertas y la de obtener acceso físico. O simplemente acceder por alguna de las redes de la institución carentes de claves de acceso, acceder por un punto físico o finalmente remitirse a los puntos de reciclaje ya que mucho del papel va integro y únicamente es reciclado en el área de servicios generales[6].

Asimismo, existen otros estudios de ataques de Ingeniería social en empresas de hidrocarburos, tal es el caso de la investigación realizada por Hernández, en 2019 donde realiza dos pruebas de ingeniería social a una empresa de hidrocarburos utilizando *Phishing* con una campaña denominada “Líderes 2019” la cual se envía a un público objetivo de 1175 personas utilizando como medio el correo electrónico. Los resultados que obtuvieron fueron que en 892 correos electrónicos se visualizaron la imagen del *Pop-up* de rastreo enviado. Otras 352 visualizaciones se realizaron por medio del formulario

[5] FIGUEROA SUÁREZ, Juan. La seguridad informática y la seguridad de la información. En: Casa editora del Polo: Revista Polo del conocimiento [en línea]. Ecuador: Casa editora del Polo, noviembre-diciembre de 2017. Ed. 14, vol. 2, nro.12. p. 3-4. [Consultado: 08 de mayo de 2021]. Disponible en https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf. ISSN: 2550-682X.

[6] BERMUDEZ PENAGOS, Edilberto. Ingeniería social, un factor de riesgo informático inminente en la Universidad Cooperativa De Colombia sede Neiva [en línea]. Trabajo de grado especialización en seguridad informática. Neiva. Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Ingeniería de sistemas. Departamento de sistemas, 2015. 116 p. [Consultado: 16 de noviembre de 2020]. Disponible en: Repositorio Educativo Digital UAO. https://repository.unad.edu.co/handle/10596/3629

del registro de la campaña y otras 76 personas diligenciaron el formulario entregando nombres, apellidos, emails corporativos, *emails* personales y teléfonos[7].

Lo anterior permite entender y visualizar el crecimiento de la ciberdelincuencia y las amenazas a medida que surgen nuevas formas de acceder a la información, por ejemplo, el uso de *phishing*, una técnica de ingeniería social que aprovecha personas incautas, con pocos conocimientos en sistemas de información y empresas que no cuentan con planes de seguridad informática bien estructurados que garanticen una correcta socialización y capacitación a sus trabajadores en temas de ingeniería social. Para combatir ataques de ingeniería social los expertos en seguridad informática y los diferentes modelos y estándares del Sistema de Gestión de la Seguridad de la Información (SGSI) han coincidido en que aparte de la seguridad de los sistemas informáticos es necesario trabajar en la capacitación periódica a empleados y personal de una empresa. Es necesario socializar información precisa y actualizada sobre los diferentes tipos de ataques y técnicas utilizadas por los ciberdelincuentes y empoderar a la persona para que esté alerta y sepa cómo enfrentar una situación encaminada a ataques de ingeniería social.

## 1.2 FORMULACIÓN DEL PROBLEMA

Teniendo en cuenta lo mencionado en los antecedentes es necesario plantear el siguiente interrogante: ¿Cuáles son las técnicas más utilizadas en correos electrónicos y redes sociales para realizar ingeniería social y extraer información de las empresas del sector financiero y entidades gubernamentales colombianas entre los años 2015 y 2020?

## 1.3 DESCRIPCIÓN

En Colombia de acuerdo con el informe de cibercrimen de la policía nacional del 20 de

[7] CORTES HERNÁNDEZ, Op. cit., p.2

octubre de 2020 se muestra que durante el 2019 los ataques informáticos de ingeniería social tuvieron un incremento en las empresas; hubo un reporte de 17531 casos, en contraste con el año 2018 se puede notar un incremento de un 54%, pudiendo conocer además que a nivel de municipios la distribución en orden de mayor a menor es Bogotá (5308), Cali (1190), Medellín (1186), Barranquilla (643) y Bucaramanga (397) casos [8].

Los principales delitos son hurto de medios electrónicos para robo de dinero con 31058 casos reportados; violación de datos personales con 8037 casos, donde el objetivo es el robo de identidad para empresas y personas; acceso abusivo al sistema informático con 7994 casos, donde buscan comprometer sistemas informáticos a través del acceso por ingeniería social; transferencia no consentida de activos con 3425 casos, encaminada a extraer dinero o transferir activos financieros de las víctimas; finalmente se encuentra el uso de *software* malicioso con 2387 casos[9].

Teniendo en cuenta el acelerado avance tecnológico que se ha impulsado con la democratización del internet y el uso de nuevas tecnologías para comunicarse, se requiere una adaptación de las empresas a los cambios sociales que les permita una mejor preparación para el uso de internet, el desempeño laboral y la seguridad de la información en la visibilizarían de sus servicios de acuerdo a sus procesos misionales, por tanto se hace necesario incluir al personal de la empresa como un ente vital y responsable en el aseguramiento y salvaguarda de la información y el papel que desempeñan en la prevención, divulgación de información confidencial y usurpación de la misma por terceros a través de técnicas de ingeniería social.

Por medio de la revisión bibliográfica se busca analizar algunas técnicas y metodologías utilizadas por los ciberdelincuentes para realizar ataques de Ingeniería social a través de correos electrónicos y redes sociales en empresas del sector financiero y entidades gubernamentales colombianas entre los años 2015 y 2020. Este material servirá de

[8] POLICIA NACIONAL DE COLOMBIA, Op. cit., p.4-17.
[9] POLICIA NACIONAL DE COLOMBIA, Op. cit., p.4-17.

insumo para producir un documento consolidado de las principales técnicas, metodologías, vulnerabilidades y amenazas, de esta manera se podrá aportar información complementaria y para uso del personal de TI y demás personas interesadas en contrarrestar o disminuir los impactos por ataques de ingeniería social. Finalmente se realizará un análisis y se evaluará el impacto que tienen los ataques en los activos e información de las empresas del sector financiero y entidades gubernamentales.

# 2. JUSTIFICACIÓN

Cada día es mayor el número de personas y empresas que manejan plataformas tecnológicas para compartir información y realizar transacciones comerciales. El crecimiento de internet hace que las empresas se conecten y transmitan información entre casi cualquier dispositivo. Las mismas que aprovechan los ciber delincuentes para atacar sistemas, una de las técnicas es la ingeniería social donde las más usadas son *Phishing* y *Baiting*, esta última consiste en dejar una USB o cd con *software* malicioso en algún lugar y esperar que por curiosidad una persona la inserte en equipo de la organización y le permita al ciberdelincuente acceder a la red y robar o atacar sistemas de información.

En las empresas los ataques de ingeniería social impactan negativamente en sus proyecciones económicas y misionales, por un lado, porque se generan pérdidas económicas por extracción de dinero y por otro porque el nivel de satisfacción disminuye por parte de los clientes ya que muchos daños de ciberataques ocurren en la información y las bases de datos de la empresa, lo cual hace que la toma de decisiones tarde mayor tiempo bien sea por falta de datos generando reprocesos o por carencia de información en la toma de decisiones y/o entrega de un servicio o producto. Lo anterior genera mala experiencia de usuario y en el peor de los casos daños irreparables afectando las finanzas de los clientes y la exposición de datos confidenciales. De allí la importancia de realizar una recopilación y análisis del impacto de las diferentes técnicas de ingeniería social usadas en Colombia, que permita conocer el estado actual de los ataques de ingeniería social y su nivel de ocurrencia por medio de correos electrónicos y redes sociales.

Este trabajo es muy importante en la medida en que se puede convertir en un insumo para alertar e informar a las personas sobre la importancia de invertir y centrarse en fortalecer las políticas de seguridad de la información abordando la ingeniería social desde la capacitación periódica a los trabajadores sobre las precauciones,

comportamientos y uso responsable de la información en las organizaciones además de suministrar herramientas básicas para enfrentar esta problemática de ingeniería social por medio de la concientización, la cautela y el uso responsable de cada persona. Asimismo, a través del análisis de la información recopilada en este documento es importante mostrar y realizar un análisis sobre el impacto que generan estos ataques de ingeniería social en las empresas y como esta afecta a la seguridad informática.

El desarrollo de este trabajo puede brindar a futuro una perspectiva a las empresas sobre seguridad informática, misma que a futuro le permitan alertarse sobre la importancia de prestar atención a la seguridad de la información desde el actuar de las personas y la privacidad frente a cada actuar, para ello la capacitación de los empleados puede mitigar el impacto de la ingeniería social. Con base a lo anterior es indispensable mostrar el comportamiento nacional y su frecuencia de ocurrencia, de ataques apoyados en ingeniería social.

# 3. OBJETIVOS

## 3.1 OBJETIVO GENERAL

Analizar técnicas y metodologías de Ingeniería social en correos electrónicos y redes sociales a partir de la revisión bibliográfica que permitan la visualización del estado actual de este tipo de ataques en las empresas del sector financiero y entidades gubernamentales colombianas entre los años 2015 y 2020.

## 3.2 OBJETIVOS ESPECÍFICOS

- Examinar información bibliográfica de las empresas del sector financiero y entidades gubernamentales colombianas con casos de ataques de ingeniería social en correos electrónicos y redes sociales para consolidación de amenazas entre los años 2015 y 2020.

- Compilar técnicas y metodologías de Ingeniería social en correos electrónicos y redes sociales de empresas del sector financiero y entidades gubernamentales colombianas que permitan la visualización de tendencias y patrones de comportamiento de los ataques ocurridos entre los años 2015 y 2020.

- Establecer las principales vulnerabilidades y amenazas que conllevan a la ejecución de ataques de ingeniería social en las empresas del sector financiero y entidades gubernamentales colombianas entre los años 2015 y 2020.

- Construir un documento con recomendaciones que consolide las principales técnicas, metodologías, vulnerabilidades y amenazas de Ingeniería social en correos electrónicos y redes sociales de empresas del sector financiero y entidades gubernamentales colombianas.

# 4. MARCO REFERENCIAL

## 4.1 MARCO TEÓRICO

La ingeniería social contempla su filosofía por así decirlo en principio fundamental y es que resulta más fácil y económico manejar a las personas que a los dispositivos electrónicos contenedores de la información. Para lograrlo los ciberdelincuentes utilizan técnicas de manipulación de la persona a nivel psicológico buscando conseguir que los usuarios revelen información confidencial o realicen cualquier tipo de acción que pueda beneficiar al ciberdelincuente. Un ciberataque de ingeniería social tiene diversos medios para realizar su propagación, pero el medio principal hoy en día a usar por parte de los delincuentes es el correo electrónico debido a que las empresas y personas lo usan de forma masiva para comunicarse y además tiene una tasa de envío de mensajes muy alta por unidad de tiempo. Aunque no es la única vía a la que acuden los ciberdelincuentes, estos pueden utilizar otros canales de comunicación entre los que se encuentran llamadas telefónicas, aplicaciones de mensajería, redes sociales, estas últimas de gran interés ya que son un espacio donde las personas convergen de forma masiva buscando para compartir cosas de la vida personal y laboral, están relajadas y el tema de seguridad es algo que no todos contemplan al hacer uso de estas plataformas.

Desde tiempos milenarios las personas han utilizado técnicas de manipulación para acceder a información confidencial y privada cuyo fin particular es poder realizar extorsiones, lograr cosas específicas y obtener información para atacar y/o lucrarse de está. Con el paso de los años y el auge de nuevas formas de comunicarse, con la llegada de las computadoras e internet, este tipo de técnicas han migrado a los medios electrónicos, donde hoy en día son muy frecuentes. Lo anterior converge con otros estudios donde se muestra que el surgimiento de nuevas tecnologías entre las que se encuentran redes sociales y correos electrónicos es el medio preferido por los ciberdelincuentes para extraer datos con mayor facilidad, pues puede llegar a un mayor

número de víctimas y por ende el éxito de obtener información se incrementa[10].

Hoy en día, el uso de dispositivos electrónicos son parte de la vida de una persona, es así como el uso de celulares inteligentes, tabletas, computadoras se convierten en la herramienta de interacción con el mundo. A esto se le suma la cantidad de tiempo que pasan las personas en internet y redes sociales, sumado a la facilidad con la cual las personas entregan información en redes sociales y en muchos casos sin ninguna configuración de privacidad, lo cual significa serviles en bandeja de plata los datos a los delincuentes.

Por citar un ejemplo las redes más usadas por los colombianos son *Facebook* y *WhatsApp*, con más de 18 millones de usuarios, seguidas por *YouTube* con 9,9 millones, *Instagram* con 7 millones y *Twitter* con 4,1 millones. Para el 2020 se estima que Colombia llegará a los 32 millones de usuarios en internet y alrededor de cinco millones usarán de manera frecuente la banca electrónica[11]. Esto muestra la gran demanda de servicios a través de plataformas electrónicas y la consecuente necesidad de ajustar los recursos tecnológicos para que sean más seguros y confiables para los usuarios que a diario utilizan este canal para realizar sus diferentes actividades. Una situación que puso a prueba el uso de los recursos tecnológicos y la seguridad de estos es la evidenciada durante la emergencia sanitaria de covid-19 de 2020 que obligo a las empresas y personas trabajar desde casa a través de internet, según El Centro Cibernético Policial[12] a través del CAI Virtual durante el 2020 atendió 11.950 incidentes y 7.862 correos gestionados donde fueron bloqueadas 5.165 páginas web, 482 portales suspendidos (9

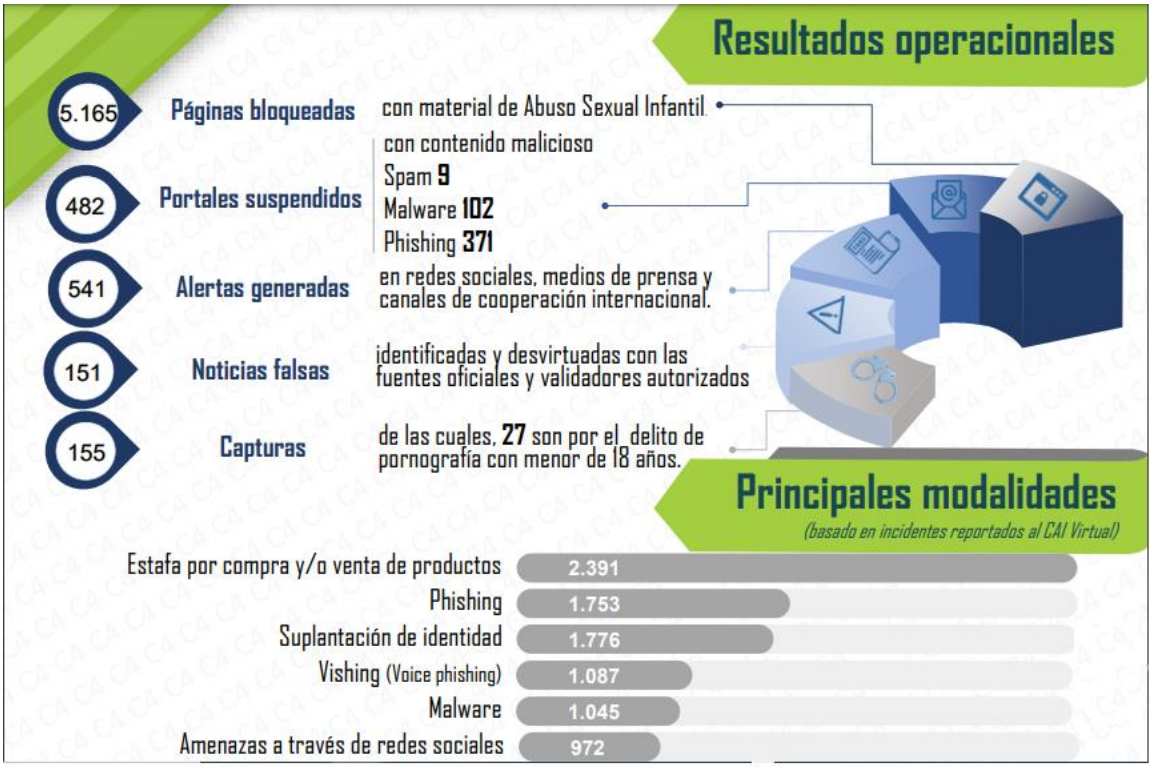
[10] LÓPEZ VILLA, Oscar David. Análisis y desarrollo de estrategias para la prevención del uso de la ingeniería social en la sociedad de la información. En: Ingenierías: Revista Ingenierías USBMed [en línea]. Medellín: Universidad de San Buenaventura, julio-diciembre de 2013. vol. 4, nro. 2. p. 1-7. [Consultado: 2 de octubre de 2020]. Disponible en http://revistas.usbbog.edu.co/index.php/IngUSBmed/article/view/287/202. E-ISSN: 2027-5846.

[11] GARCÍA, Constanza. Economía digital [en línea]. BBVA. Colombia. (19 de septiembre de 2019). [Consultado: 2 de octubre de 2020]. Disponible en: https://www.bbva.com/es/co/colombia-llegara-a-los-32-millones-de-usuarios-de-internet-en-2020/

[12] POLICIA NACIONAL DE COLOMBIA [sitio web]. Bogotá. CAI VIRTUAL. Balance Cibercrimen 2020. [Consultado: 18 de mayo de 2021]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

*spam*, 102 *malware*, 371 *phishing*) tal como se muestra en la **Figura 1.**

**Figura 1.Operaciones realizadas por infracciones a la ley 1273 en colombia durante el 2020.**



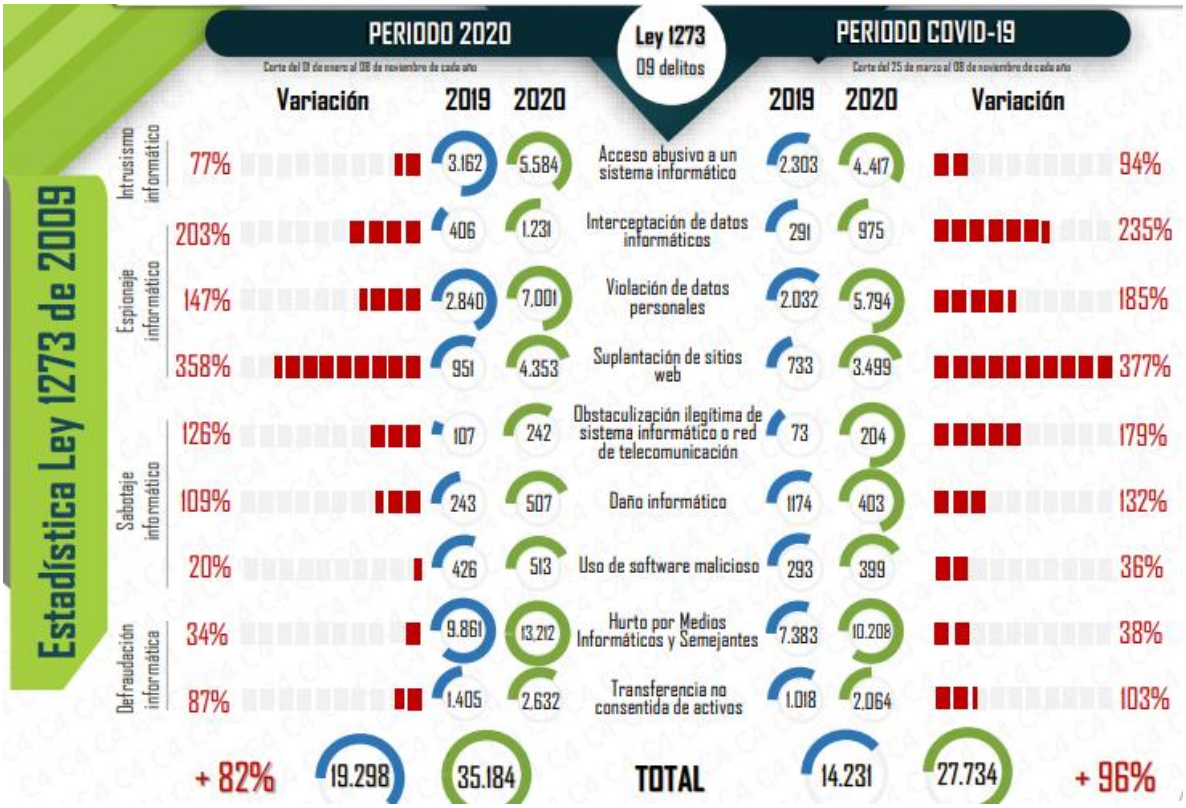

Fuente: https://bit.ly/3vTSxpk

Estos ataques cibernéticos están penalizados por el convenio de Budapest a nivel internacional y en Colombia por la ley 1273 de 2009, para el 2020 claramente hubo un incremento tal como se muestra con la **Figura 2** dentro de los nueve delitos evaluados por el CAI Virtual de la policía nacional[13], durante el periodo COVID-19 los casos de ataques informáticos donde mayores violaciones se presentaron son la suplantación de sitios web e interceptación de datos informáticos con 2766 y 684 casos respectivamente. Se puede notar que el escenario elegido por los ciberdelincuentes para atacar es aquel que para la fecha más usuarios demandaba y esto es porque muchas empresas tuvieron

[13] Ibid., p.1

que abrir nuevas formas para ejercer el comercio y las comunicaciones de la empresa y sus colaboradores a través de internet, lo cual pudo dejar al descubierto ciertas falencias en materia de seguridad de las plataformas utilizadas o de la falta de capacitación del talento humano de las empresas y el afán de establecer nuevas formas de comunicarse.

**Figura 2. Reporte de cibercrimenes a la ley 1273 en colombia durante el 2020.**

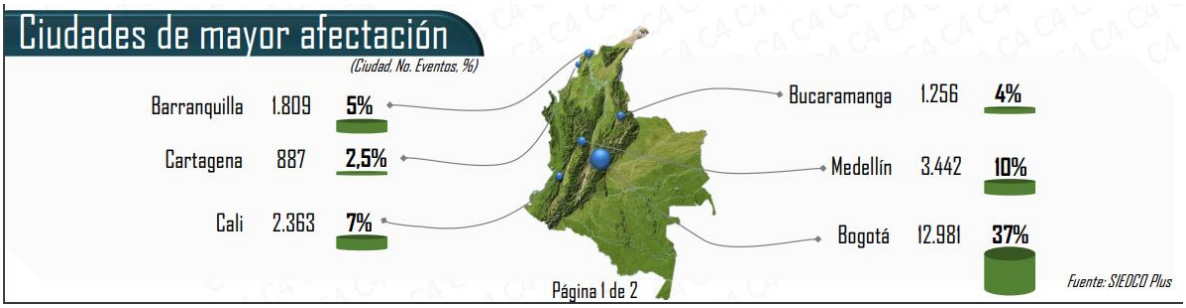



Fuente: https://bit.ly/3vTSxpk

En Colombia las ciudades más grandes son Bogotá, Medellín, Cali y Barranquilla asimismo son las que albergan el mayor número de empresas, las mismas que se encuentran consumiendo servicios de internet para el desarrollo de alguna o varias actividades comerciales y que para época de pandemia incrementaron la demanda de servicios digitales e internet para poder compensar de alguna forma la crisis generada por la pandemia de COVID-19, es así como en la **Figura 3** se observa que Bogotá es la ciudad que recibe el 37% de los ataques, seguido de Medellín y Cali con el 10% y 7%

respectivamente[14].

**Figura 3. Afectación de cibercrimenes por ciudades colombianas durante el 2020.**




Fuente: https://bit.ly/3vTSxpk

Por otro lado, está el ataque a correos electrónicos, donde el posicionamiento de las tecnologías de la información trajo consigo la migración de muchos servicios transaccionales a internet, donde los delincuentes aprovechan este cambio para camuflarse como prestadores de servicios bancarios e intentar apoderarse de datos de clientes incautos y generar robos de dinero y vaciar cuentas. Esta técnica la direccionan a través de correos electrónicos mediante el envío de mensajes (*SMiShing*), para que la estrategia sea más provocativa y la victima sean tentada a acceder a sus peticiones, usan promociones y falsos premios. Para lo cual el usuario "ganador" debe enviar información o llenar formularios para hacer efectiva la entrega de la promoción o premio[15].

A priori, se puede pensar que esta nueva forma de interactuar entre las personas se debe hacer de manera concienzuda, ya que, si se analiza por el lado de las redes sociales, estas conectan gran cantidad usuarios y esto hace que se comparta los gustos, fotos, actitudes, hobbies, necesidades, etc., con cualquier cantidad de personas, donde no todas tiene buenas intenciones con su perfil, puede estar en riesgo su privacidad y la de su empresa. A su vez el posicionamiento del correo electrónico como el nuevo canal de comunicación, conlleva a ser blanco de ataques y donde se puede decir que esta técnica

[14] Ibid., p.2
[15] LÓPEZ VILLA, Op. cit., p.2.

debe su éxito y conservación a través del tiempo porque aprovecha la ingenuidad de las personas y/o confianza para acceder a datos confidenciales de la red sin necesidad de atacar sistemas robustos.

Además, como lo manifiesta Salvador, 2011, la ingeniería social es muy exitosa debido a los bajos costos y un alcance enorme de forma simultánea donde el *phishing*[16] y esto está enlazado con una de las connotaciones que tienen los piratas informáticos es que la debilidad en las personas se puede traspasar fácilmente por lo cual el uso de ingeniería social es el camino propicio[17].

Lo anterior se complementa con lo manifestado por Romero en el trabajo denominado "el arte de la ingeniería social, donde relaciona las diferentes herramientas que existen para asegurar un sistema de información" entre las que están *firewalls*, IDS (Sistemas de detección de intrusos), IPS (Sistemas de protección de intrusos); los cuales requieren de altas inversiones y el apoyo de personal especializado y experimentada[18]. Situación que a los administradores de empresas les parece costoso y dispendioso de implementar, razón por la cual muchas empresas carecen de un sistema de seguridad informática lo cual pone en riesgo la confidencialidad, integridad y disponibilidad de la información.

En cuanto a la seguridad de la información del área gerencial y las redes sociales el trabajo de Gregorio Arévalo denominado "Redes sociales digitales: Una Aproximación a

[16] DE SALVADOR, Luis. Ingeniería Social y Operaciones psicológicas en internet [en línea]. Ieee.es. (18 de octubre de 2011). [Consultado: 2 de octubre de 2020]. Disponible en Internet: http://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO74-2011.IngenieriaSocial_LuisdeSalvador.pdf

[17] TORRES DIAZ, Oswaldo Alejandro. Diseño e implementación de un plan de concientización frente a la ingeniería social para la empresa promociones y cobranzas beta s.a. [en línea]. Trabajo de grado para optar al título de Especialista en Seguridad Informática. Bogotá. Universidad Piloto de Colombia. Facultad de posgrados de ingeniería. Departamento de sistemas, 2017. 188 p. [Consultado: 2 de octubre de 2020]. Disponible en: Repositorio Educativo Digital UNIPILOTO. http://repository.unipiloto.edu.co/handle/20.500.12277/2769

[18] ROMERO RUBIO, Diego Alexander. El arte de la ingeniería social [en línea]. Trabajo de grado Especialización de seguridad informática. Bogotá. Universidad piloto de Colombia. Facultad de ingeniería. Departamento de sistemas, 2019. 10 p. [Consultado: 2 de octubre de 2020]. Disponible en: Repositorio Educativo Digital UNIPILOTO. http://repository.unipiloto.edu.co/handle/20.500.12277/6354

los riesgos en sistemas de información gerencial" muestra algunos casos de ataques en Colombia, entre los que se encuentran: Un ataque a la Universidad Surcolombiana en el 2018 por parte de seis estudiantes quienes accedieron durante el periodo vacacional al registro de notas y modificaron 366 calificaciones; asimismo está el ataque a los correos electrónicos de los candidatos a la rectoría den la Universidad Nacional de Colombia enfocada a sustraer información y divulgar mensajes para dañar la imagen de los candidatos. Al mismo tiempo que cita la importancia de proteger los sistemas en instituciones de educación superior y la necesidad de conservar en el tiempo la información y contrarrestar los ataques de ingeniería social por medio de políticas y planes de protección unido a procesos continuos de capacitación[19].

Profundizando un poco más en los diferentes tipos de ataques están:

- **Ataque telefónico.** Relacionado con llamadas a través de teléfono celular ofreciendo algún servicio o beneficio con el objeto de extraer información del cliente de manera remota y mediante el engaño.

- **Ataques web.** Robo de información a través del uso de páginas web servidas a través de correo electrónico, redes sociales, chats y cualquier plataforma con acceso a internet. Son ataques que emulan un servicio de un banco, supermercado, sitio de ofertas de internet etc. por ejemplo, atrayendo la atención de sus víctimas, por medio del trabajo de expertos quienes usan técnicas avanzadas y también el aprendizaje empírico producto de la práctica del ejercicio delictivo.

- **Mirar por encima del hombro (*Shoulder surfing*).** Consiste en espiar en forma presencial a un usuario para copiarle la contraseña y usuario, por eso se llama

[19] ACOSTA, Op. cit., p.2.

mirar por encima del hombro, y consiste en mirar como la persona teclea y capturar visualmente sus datos[20].

- **Recolección en reciclaje (*Dumpster diving*).** Revisión de los documentos desechados íntegramente en el tarro de la basura con el fin de encontrar datos sensibles[21].

Lo anterior dependiendo del grado de complejidad y conocimiento se pueden clasificar en dos grupos:

- **Interacción activa.** Ataque de ingeniería social realizado por personas con conocimiento empírico o el instinto. La cual se va mejorando en el atacante con el paso del tiempo[22].

- **Interacción pasiva.** Ataque de ingeniería social realizado por personas capacitadas con conocimiento de técnicas, conceptos, y el establecimiento de patrones que permitan optimizar el ataque[23].

Con base en lo anterior y teniendo el ataque en su desarrollo se debe tener en cuenta varios criterios entre los que se encuentran que debido a la evolución constante este tipo de ataques de ingeniería son más organizados, se han estructurado y trabajan de forma más metódica, dando paso una serie de fases y que se pueden describir a continuación:

- **Reconocimiento.** Etapa durante la cual se recopila información correspondiente

[20] GOMÉZ VIEITES, Op.cit., p.132.
[21] GOMÉZ VIEITES, Op.cit., p.132.
[22] SERGIO ARCOS, Sebastián. Ingeniería social: Psicología aplicada a la seguridad informática [en línea]. Trabajo de grado Ingeniería en Informática. Barcelona. Universidad Politécnica de Cataluña. Facultad de Ingeniería. Departamento de Ingeniería de Servicios y Sistemas de Información, 2011. 142 p. [Consultado: 25 de septiembre de 2020]. Disponible en: Repositorio Educativo Digital UPC. http://hdl.handle.net/2099.1/12289
[23] Ibid., p.7

a datos de personas, números de contacto para lo cual se usan fuentes de datos entre las que se encuentren redes sociales, buscadores web, contacto con personas, llamadas telefónicas.

- **Exploración.** A partir de la información recopilada en la fase de reconocimiento se hace un escaneo más profundo contra el sistema a atacar por ejemplo se pueden escanear vulnerabilidades en puertos, nombres de dominio y direccionamiento IP de la red, entre otros.

- **Obtención de acceso.** Corresponde a la fase en la cual el atacante logra ingresar a un sistema valiéndose de claves y demás vulnerabilidades encontradas en el sistema atacado. Una vez el atacante es un usuario con todos los privilegios puede retomar la recolección de información[24].

- **Conservación de acceso.** Para esta fase y con el objetivo de mantener el acceso al sistema, los atacantes realizan la instalación de programas, *script*s y demás *software* que permite mantener el enlace mientras se realiza el ataque para robo de información del sistema atacado.

- **Eliminación de rastro.** Finalizado el ataque, se busca borrar cualquier huella en el sistema para evitar su detección sino su actividad será infructífera. Para ello el atacante puede camuflar su dirección IP y borrar cualquier traza que alerte al administrador del sistema detecte la intrusión[25].

Del mismo modo teniendo en cuenta el grado de especialización de los ataques se pueden denotar algunas técnicas entre la que se encuentran:

[24] OLIVARES SERRANO, Javier. Seguridad informática: Hacking Ético. [en línea]. 4 ed. Barcelona: Ediciones ENI. 2018, 810 p. [Consultado el 25 de septiembre de 2020]. Disponible en: https://catoute.unileon.es/permalink/34BUC_ULE/1ekdeev/alma991000306699705772. Epsilon.ISBN: 978-2-409-01297-6.
[25] Ibid., p.52

- *Baiting*:
- *Phishing*
- *IVR o Phone Phishing*
- *Quid Pro Quo*
- Pretexting
- *Farming*

De las anteriores el *Baiting* y el *Phishing* son las técnicas más utilizadas, la primera que consiste en dejar un dispositivo de almacenamiento externo que puede ser una memoria USB o CD con *software* malicioso en algún sitio dentro de la organización y esperar a que alguna persona la recoja e inserte en algún equipo de cómputo para mirar que contiene y en ese momento se ejecuta un código malicioso que le permite al ciberdelincuente acceder a la red y a la información de la víctima mediante el uso de ataques a las plataformas. En algunos estudios como los de Hernández se muestra un experimento que consistió en diseñar una tarjeta USB con el logo de un proveedor de internet para ganar confianza e incrementar la efectividad e internamente lleva un archivo malicioso con un nombre muy atractivo para la víctima "internet gratis, lo cual corresponde y tiene relación entre los logos de la tarjeta USB y el contenido interno situación que conlleva a la víctima a pensar que es seguro y coherente de utilizarlo sin ningún peligro. Al final del experimento se encontró que de las 40 tarjetas que se dejaron en zonas públicas de la organización 35 fueron tomadas por personas de las cuales 7 fueron entregadas área de tecnología y los 28 restantes cumplieron su cometido ya que fueron ingresadas por las personas a los equipos corporativos y ejecutaron el *software* malicioso y enviaron la información al servidor[26]. Mientras que el *Phishing* se dedica a la suplantación de correos y páginas de grandes empresas para obtener información sensible, la cual es entregada por las personas al caer en el engaño y la urgencia que les

[26] CORTES HERNANDEZ, Andrés. Ingeniería social: *Phishing* y *Baiting* [en línea]. Trabajo de grado Especialización en Seguridad Informática. Bogotá. Universidad Piloto de Colombia. Facultad de ingenierías. Departamento de sistemas, 2019. 10 p. [Consultado: 2 de octubre de 2020]. Disponible en: Repositorio Educativo Digital UNIPILOTO. http://repository.unipiloto.edu.co/handle/20.500.12277/6349

imprimen de actuar rápido para no poner en peligro sus operaciones en internet.

## 4.2 MARCO CONCEPTUAL

**4.2.1 Definición de conceptos.** A continuación, se relacionan algunos conceptos que son de interés para la compresión del tema que aborda esta monografía.

**4.2.1.1 Ingeniería social por *Baiting*.** Es muy parecida al *phishing* y se aprovecha de los internautas para obtener información entre las que están, credenciales de acceso y demás información bancaria por medio de grandes promociones, obsequios o revisar noticias o sucesos impactantes. Existen diferentes métodos entre los que se encuentran:

- Disparar anuncios mientras el usuario navega en internet con enlaces que llevan a entornos ficticios y que piden información sensible.

- Dejar en un lugar público un dispositivo extraíble infectado (memoria USB o Cd) que contenga un virus o *malware* y con el cual se busca que una persona lo recoja y lo conecte a los equipos de una compañía[27]. Una vez la víctima lo conecte a una computadora para revisar el contenido el *malware* iniciara su instalación y ejecución e infectara con *software* malicioso para extraer datos o dañar el sistema.

**4.2.1.2 Tipos de correos electrónicos.** De acuerdo con el tipo de cuenta existen dos cuentas de correo electrónico, estas son:

- Correo personal. Son cuentas creadas para uso personal y usar para comunicarse con otras personas y navegar en la web, son gratuitos, con algunas restricciones y manejan como dominio el del proveedor de correo (ej. @gmail.com).

[27] LÓPEZ GRANDE, Op.cit., p.40.

- Correo corporativo. Son cuentas creadas para uso empresarial, son de pago y manejan un dominio personalizado de la empresa contratante (ej. @miempresa.com). Estas cuentas poseen copias de seguridad a su vez que permiten mayor seguridad y control de las organizaciones en el manejo de la información pudiendo sincronizarse con calendarios, chats, videoconferencias, contactos, control de tareas y *suite* ofimática dependiendo del plan contratado. Además de permitir en algunos casos la sincronización para recibir en el buzón del correo mensajes de redes.

La comunicación electrónica se ha popularizado en todos los niveles y organizaciones y, entre sus géneros, el correo representa, en la actualidad, una de las aplicaciones informáticas más utilizadas, práctica social que ha sustituido, en gran medida, a la carta, al fax o al teléfono[28].

**4.2.1.3 Ataques *Pharming*.** Este tipo de ataque resulta de la combinación de dos técnicas, el *farming* y el *phishing* y su objetivo es robar información sensible por medio de la interceptación y manipulación del tráfico web. Para interceptar la información en la navegación web los ciberdelincuentes pueden insertar *malware* que modifica el archivo hosts en los equipos locales o atacar a los servidores DNS para que estos no puedan convertir correctamente a la IP de cada dirección web que usan los servidores DNS para identificar a cada una de computadoras conectadas en internet. En el primer caso al modificar el archivo hosts del sistema operativo de la computadora de la víctima se logra que el equipo envíe datos a otro sitio web falso. En el segundo caso al alterar el funcionamiento del DNS los paquetes se desvían a otros equipos falsos sin que la víctima logre identificarlos ya que esto ocurre después de enviar la petición de conexión al DNS. Respecto a este tipo de ataques en lo que copete al usuario es importante usar *software*

[28] LÓPEZ ALONSO, Covadonga. El correo electrónico. En: Estudios de lingüística del español [en línea]. Covadonga López Alonso: Universidad Complutense de Madrid, enero-junio de 2006. vol. 24. p. 1-3. [Consultado: 30 de septiembre de 2020]. Disponible en https://www.raco.cat/index.php/Elies/article/view/195637

licenciado y mantenerlo actualizado, instalar antivirus y demás programas *antimalware*, y algo muy importante manejar las cosas con cautela analizando cada acción que se realice en un dispositivo electrónico, antes de instalar o hacer clic a un enlace en internet verificar si es confiable debido a que los ciberdelincuentes ponen cebos muy atractivos para que la persona actúe de emoción y no con la razón. Estos ataques buscan rápidamente ganarse la confianza de la víctima y esto lo logran por medio de una previa investigación de su comportamiento en redes sociales u otro medio con información expuesta.

**4.2.1.4 Ataques de Ingeniería social**. El concepto de ingeniería social es utilizado para referirse a una serie de técnicas y trucos utilizados por delincuentes informáticos para sustraer información confidencial y sensible de las personas y/o empresas de un sistema informático en particular mediante el engaño, la manipulación, la empatía, el convencimiento, la confianza y la persuasión[29]. Incluso muchos usuarios no son precavidos al momento de entregar información, lo hacen sin ningún problema, es más a muchos no les interesa el manejo de sus datos, lo único que les interesa es poder acceder a ciertas recompensas u obtener acceso a una cuenta en internet o recibir algún obsequio o promoción en particular. Estás técnicas con el paso del tiempo se mantienen e incluso han evolucionado y se han convertido en formas más elaboradas, haciendo uso de modelos psicológicos y habilidades sociales tal como lo manifiesta Sánchez en el trabajo denominado Ingeniería social, una técnica subestimada por desconocimiento[30]. Esto es algo que comparto ya que a los diferentes ataques de ingeniería les incluyen análisis de personalidad, técnicas de persuasión, componendas a forma de guion que concuerdan completamente e incluso con datos personales del núcleo cercano de la víctima por lo cual el usuario no puede notar que se trata de algo extorsivo. A estas técnicas de ingeniería social incluso hoy en día le aplican estrategias de *marketing* y *neuromarketing*.

[29] GOMÉZ VIEITES, Álvaro. Enciclopedia de la Seguridad Informática. Segunda edición. Madrid, España: Editorial RA-MA. 2017. 1085 p. ISBN: 9788499640385.

[30] SANCHEZ, PATARROYO, Henry. Ingeniería social, una técnica subestimada por desconocimiento [en línea]. Trabajo de grado Especialización en Seguridad Informática. Bogotá. Universidad Piloto de Colombia. Facultad de ingenierías. Departamento de sistemas, 2016. 8 p. [Consultado: 25 de septiembre de 2020]. Disponible en: Repositorio Educativo Digital UNIPILOTO. http://repository.unipiloto.edu.co/handle/20.500.12277/4934

Dentro de las técnicas de recolección de información antes del ataque usadas en ingeniería social se pueden encontrar las siguientes:

- **Pasivas.** Técnica que se enfoca en la evaluación de la rutina de una persona y en la documentación de cada una de sus actividades a partir de la observación información que luego permite realizar un perfil psicológico de la víctima.

- **Presenciales.** Técnica que se enfoca en la evaluación de las víctimas de manera directa con la persona de forma física y apoyándose en la confianza e ingenuidad de las personas. Dentro de la cual se encuentran las técnicas presenciales no agresivas para las cuales se utilizan como estrategia *Shoulder surfing*, *Dumpster diving* y seguimiento a personas. Por otro lado, las técnicas presenciales agresivas utilizan como estrategia la Extorsión, presión psicológica, suplantación de identidad o *phishing*, *spear phishing*, *Pharming*.

- **No presenciales.** Técnica que se enfoca en la obtención de información de forma remota utilizando como herramientas de enlace con la victima correos electrónicos, teléfonos, *SMS Phishing*, *Voice Phishing*. A nivel de técnicas de ingeniería social la que mayormente se usa es a través de correos electrónicos y redes sociales es el *phishing*.

**4.2.1.5 Ataques por *Phishing*.** De las técnicas más viejas y efectivas centrada en generar influencia a través de correos suplantados de empresas influyentes para extraer información sensible. *Phishing*. El término *phishing* proviene de la palabra fishing que traduce pescar por lo que el método de ingeniería social por medio de *phishing* se basa en lograr que un usuario caiga en la trampa, así como un pez muerde el anzuelo en cuyo fin por parte del atacante se encuentra el poder obtener usuario y contraseña[31]. Se encuentran entre otros los siguientes tipos de ataque por medio de *phishing*:

[31] CARRILLO LUQUE, Op.cit., p.55-57.

- ***Phishing* de lanza o de objetivo específico.** Estrategia realizada por medio de correo electrónico, redes sociales profesionales y que se encuentra enfocada en detectar inicialmente las vulnerabilidades de una empresa para conseguir una víctima que pueda brindarles el acceso a acciones específicas dentro de la misma. Para ello los atacantes buscan personas de entornos administrativos y gerenciales que cuenten con escasos conocimientos de TI (Tecnología de la información) pero que tengan a la mano datos de acceso a los sistemas de la institución.

- ***Phishing* de redirección o clonado.** Hace uso de la publicidad enviada por medio de correo masivo para engañar a las víctimas y lograr la recopilación de información por medio de formularios web. Estas estrategias publicitarias están camufladas en correos de personas conocidas o empresas de nombre reconocido que para entregar un premio solicitan suministrar información confidencial. Asimismo, es típico el correo electrónico con mensajes de alerta sobre supuestos bloqueos a medios electrónicos y que piden ingresar información para no perder la capacidad de usar servicios y/o productos financieros.

- ***Phishing* de estafa o fraude.** Hace uso del correo electrónico, redes sociales y servicios de mensajería personalizado y ocasional para engañar a las víctimas y lograr establecer contacto para entablar conversación y ganar la confianza de su víctima. Una vez logra aprovechar las debilidades de la persona procede el delincuente a pedirle que realice transacciones o acceda a permitirle ingresa a datos privados como fotos con las cuales después chantajeará a la persona o la obligará a entregar sumas de dinero para no divulgar información sensible.

- ***SMS Phishing*.** Para llegar a sus víctimas esta técnica hace uso del correo electrónico y los mensajes de texto[32]. Siendo estos últimos de gran uso hoy en día

[32] CARRILLO LUQUE, Vicente y SÁNCHEZ PASTOR, Fernando. La ingeniería social aplicada al delito informático. una aproximación [en línea]. Universidad Complutense de Madrid. Facultad de informática. Departamento de Sistemas Informáticos y Computación, 2011. 57 p. [Consultado: 24 de septiembre de 2020]. Disponible en:

debido a que carecen de doble factor de autenticación y hacen más fácil la entrega de contenidos o mensajes para engañar a las personas. Caso contrario ocurre con los correos electrónicos o mensajería ya que cada día tienen mayores niveles de seguridad y factores de autenticación más eficientes como lo son la huella o doble contraseña.

- ***Voice Phishing*.** Para llegar a sus víctimas esta técnica hace uso de las llamadas de voz para emitir sus mensajes y entablar conversación más directa[33]. Para esto usan un discurso convincente y sustentado en la presión y la urgencia por ejemplo una persona llama a su teléfono manifestado que un familiar fue arrestado o sufrió un accidente y necesitan urgente una suma de dinero para ayudarle. Otra técnica es camuflándose como empresas de telefonía que ofrecen paquetes de minutos o datos los cuales para hacerse efectivos es necesario extraer la *simcard* del dispositivo por un lapso, espacio en el cual llaman a otro familiar para infórmale que tienen secuestrado a su familiar y como no es posible ubicarlo por llamada a su número personal las víctimas entregan cifras de dinero solicitadas.

- **IVR o Phone *Phishing*.** Hace una copia del sistema de respuesta de voz interactiva de una empresa relevante e influyente a través de un número telefónico buscando sacarle información sensible de sus cuentas bancarias[34].

**4.2.1.6 Pasos de ataques *phishing*.** Un proceso exitoso para los atacantes debe cumplir al menos las siguientes actividades.

- Análisis de las personas que son susceptibles de ataque.

http://www.simuladoronline.es/descargas/La_Ingenieria_social_Aplicada_al_Delito_Informatico_Una_Aproximacion.pdf

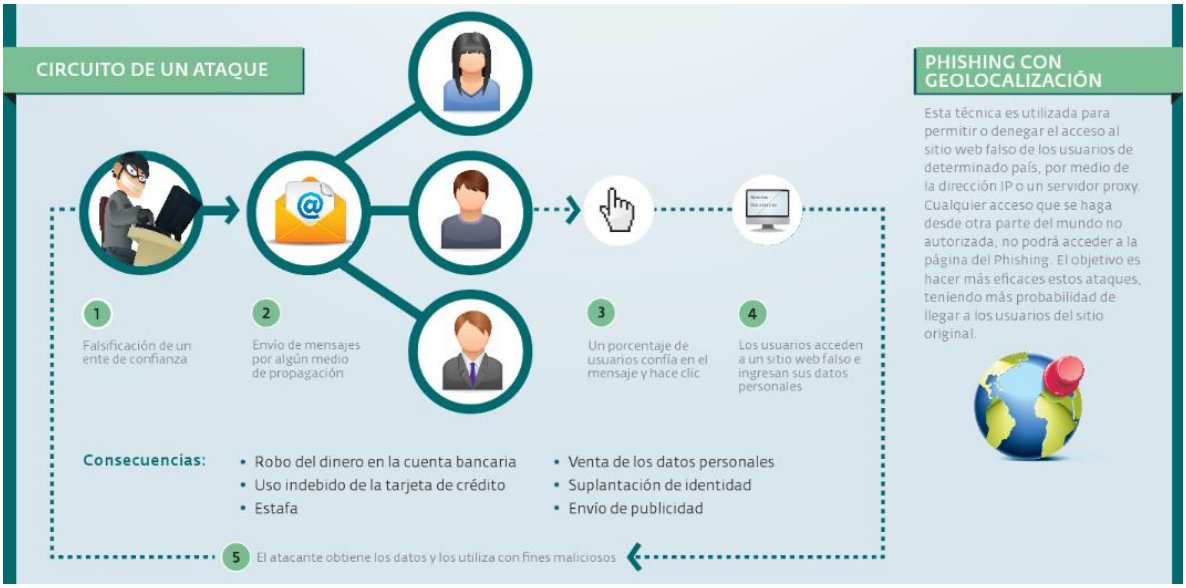
[33] CARRILLO LUQUE, Op.cit., p.55-57.

[34] LÒPEZ GRANDE, Carlos et al. Ingeniería social: El ataque silencioso. En: ITCA-FEPAD [en línea]. El salvador: Revista Tecnológica de Escuela Especializada en Ingeniería, enero-diciembre de 2015, vol., 2, nro. 8. 8 p. [Consultado: 7 de octubre de 2020]. Disponible http://hdl.handle.net/10972/2910.

- Planeación del momento a desplegar el ataque y el estudio de la empresa a suplantar mediante una campaña publicitaria.
- Diseño y montaje de la estrategia de ataque.
- Ejecución del ataque.
- Esperar que los formularios de ataque sean diligenciados con la información requerida.

Dentro de las cuales de acuerdo con la ejecución de un ataque por *phishing* ocurren una serie de pasos tal como se muestra en la **Figura 4,** teniendo encuentra la técnica *Password Harvesting* (cosecha y pesca de contraseñas), la cual inicia con el envío de un correo electrónico suplantado utilizado la imagen y formatos de una empresa de confianza o de uso frecuente de la víctima. Una vez se obtiene su atención se usan técnicas de manipulación donde se transmite sentido de urgencia y el miedo de perder servicios o productos si no se realiza urgentemente los ajustes solicitados.

**Figura 4. Pasos para ejecución de *phishing***




Fuente: http://hdl.handle.net/10234/127507

En síntesis, con lo anterior autores entre los que se encuentran Leguisamon[35] suponen que existen unas etapas bien diferenciadas respecto a los ataques por *phishing* y que se pueden desplegar durante un ataque al menos las siguientes:

- **Planificación.** Etapa durante la cual el delincuente informático define el personal objetivo de los ataques a perpetrar, el tipo de información que desea extraer (cuentas de usuario y contraseñas, datos bancarios o personales) así mismo define cuáles serán las mejores herramientas para usar durante el proceso de ataque y los nombres de empresas sobre las cuales se va a camuflar ante sus víctimas. También es una etapa sobre la cual se verifica y decide como se proyectará el ataque si de forma individual o masiva. De otro lado se evalúa el rol que desempeñara la víctima durante todo el proceso de ataque y se verifica la infraestructura necesaria para lograr su cometido. A partir de estas decisiones se puede encajar el ataque en tres tipos de *phishing*:

    a) Alta complejidad/ Baja colaboración (Ej. ataque a servidor DNS) víctima.
    b) Media complejidad/ Media colaboración (*malware*).
    c) Baja complejidad/ Alta colaboración víctima (correo electrónico).

- **Preparación.** Se planea de acuerdo con la complejidad descrita en el paso anterior. Es la etapa durante la cual se afinan las herramientas y técnicas para ejecutar el ataque de manera efectiva y conseguir el objetivo trazado en el primer paso denominado planificación. Esta etapa en gran medida tiene que ver con la efectividad de un ataque pues es el espacio donde se delimita e incorporar mecanismos que incrementen la efectividad y se reduzcan los porcentajes de error.

- **Ataque.** Es la etapa donde se lanza la campaña a través de correo electrónico, redes sociales u otro canal interactivo buscando acciones específicas de la víctima, las

[35] LEGUIZAMON, Maira Sheila. El *Phishing* [en línea]. Trabajo final de grado en criminología y seguridad. Castellón de la Plana. Universidad Jaime I. Escuela Superior de Tecnología y Ciencias Experimentales. Departamento de Lenguajes y Sistemas Informáticos, 2015. 47p. [Consultado: 10 de septiembre de 2020]. Disponible en: Repositorio Educativo Digital UJI. http://hdl.handle.net/10234/127507

cuales van a depender del tipo *phishing* utilizado y el nivel de participación, donde pueden ser dependientes o no de la acción de la víctima. Por lo que esta etapa requiere tratamientos diferentes donde los tiempos de respuesta y el porcentaje de recaudo de la información también varían. Además, existe un factor determinante en la ejecución del ataque y es la seguridad de las plataformas electrónicas respecto a *spam* y correo no deseado la cual cada día es más efectiva.

Para aprender a identificar estos ataques OSI[36] tiene algunas recomendaciones entre las que se detallan:

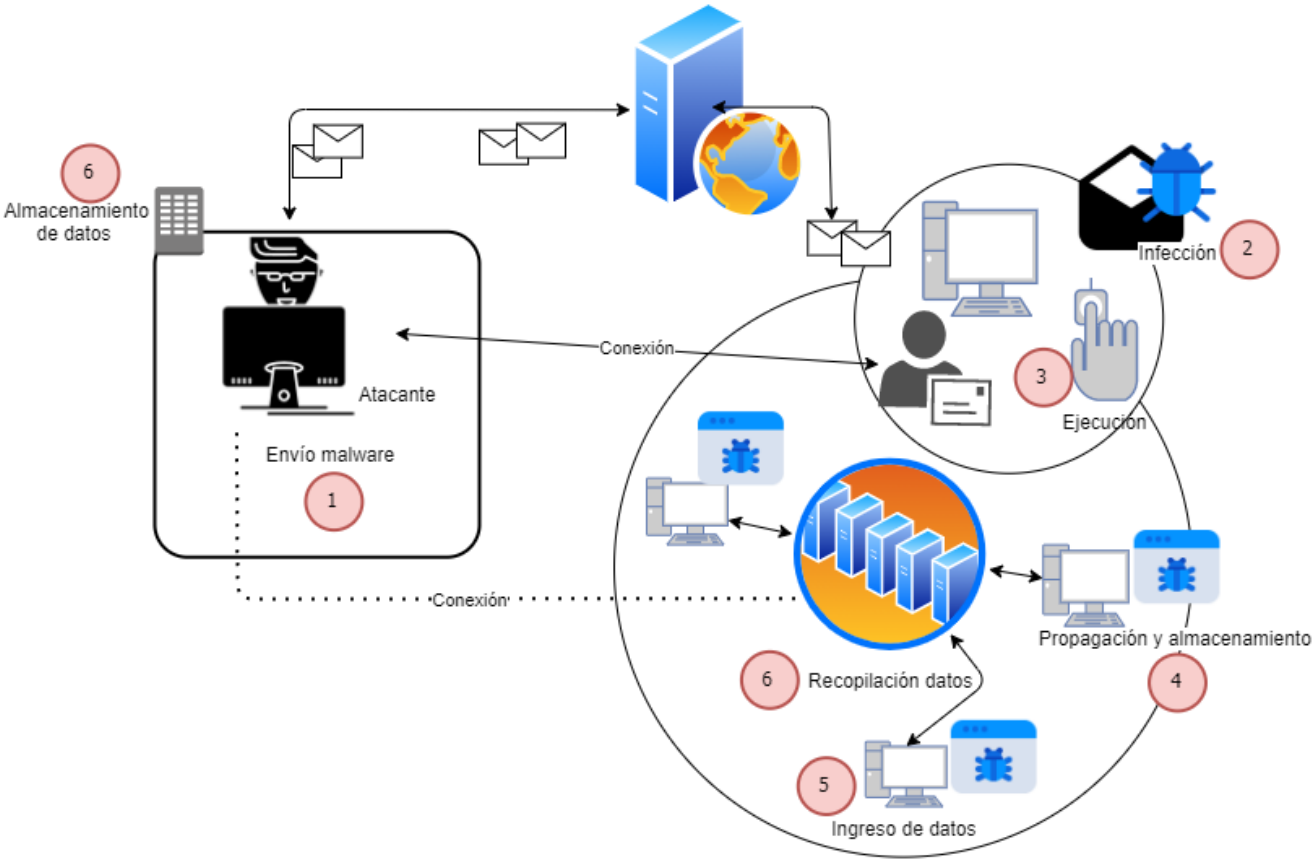
- Comprobar ortografía y redacción de los correos además de coherencia en el mismo.
- Verificar que la cuenta es original y no provenga de cuentas con dominio público
- Revisar la *URL* y asegurarse que redirige al mismo sitio y no a otro extraño.
- No descargar archivos adjuntos si no puede comprobar o estar seguro del remitente.

De otro lado existen otro tipo de ataques que usan programas maliciosos o más conocidos como *malware*[37] que realizan acciones dañinas sin consentimiento del usuario en un sistema operativo o *software* determinado pero que si requieren la intervención del usuario en alguna etapa del proceso (descarga y/o ejecución), por ejemplo aquellos ataques *phishing* para tener éxito requieren de la correcta ejecución de cada uno de los pasos que se muestra en la **Figura 5**, si por algún motivo la victima recibe el correo electrónico con el *malware*, lo descarga, pero no ejecuta los demás procesos se verían afectados y la extracción de información no se podrá ejecutar. En este caso se está hablando de un caso de *phishing* de media complejidad y media colaboración y posee

[36] OSI. Aprendiendo a identificar fraudes *online* [sitio web]. España; [Consultado: 06 de agosto de 2021]. Disponible en: https://www.osi.es/es/guia-fraudes-online
[37] KASPERSKY, CENTRO DE RECURSOS. Virus informáticos y *Malware* [sitio web]. América latina; [Consultado: 07 de mayo de 2021]. Disponible en: https://latam.kaspersky.com/resource-center/threats/computer-viruses-and-malware-facts-and-faqs

dos momentos importantes el primero cuando el *malware* infecta el sistema por medio de la ayuda de la víctima y el segundo cuando se ejecuta en la maquina a infectar el código malicioso.

**Figura 5. Ataque por *Phishing* a través de *malware***




Fuente: Propia adaptado de http://hdl.handle.net/10234/127507

- **Recolección de datos.** Dependiendo de nivel de éxito del proceso anterior y la capacidad de respuesta de la víctima y su grado de participación o no este proceso será rápido o lento. Es decir, la recolección de información está ligada al tipo de estrategia *phishing* descrita en el primer paso denominado Preparación, consideraciones que se pueden evidenciar en la **Tabla 1.**

**Tabla 1. Agentes y tareas de acuerdo con los niveles de participación y complejidad de un ataque *Phishing.***

| | Agentes | Tareas |
|---|---|---|
| **Alta complejidad Baja participación** | • *Phisher* y colaboradores<br>• Empresa atacada<br>• Victimas | • A la espera de los datos<br>• Ejecución de código malicioso |
| **Media complejidad Media/Alta participación** | • *Phisher* y colaboradores<br>• Empresa suplantada (Si existe)<br>• Victimas | • A la espera de los datos (aplicaciones autónomas y *Phishing* de motor de búsqueda)<br>• Ejecución de códigos maliciosos para la consecución de datos (robo de datos *Pharming*) |
| **Baja complejidad Alta participación** | • *Phisher* y colaboradores<br>• Empresa suplantada<br>• Victimas | • A la espera de los datos (vía respuesta correo electrónico o visita a la web fraudulenta) |

Fuente: Propia, adaptado de http://hdl.handle.net/10234/127507

- **Ejecución del fraude.** Si el delincuente informático ha llegado a esta fase con información se puede decir que para este las anteriores fases (planificación, preparación, ataque y recopilación) fueron un éxito y ahora puede realizar lo que tenga a consideración con la información de sus víctimas.

- **Post ataque.** En esta fase el delincuente informático busca borrar rastros y evitar dejar huella en el sistema con las cuales pueda ser rastreado y/o detectado y poner en riesgo su actividad fraudulenta. Aquí por ejemplo el atacante intenta cambiar registros de las direcciones MAC, esconder o modificar su dirección IP y borrar cualquier traza que pueda alertar al administrador del sistema atacado.

**4.2.1.7** ***Pretexting*****.** Es un ataque donde el atacante crea un escenario ficticio creíble y muy natural para ganarse la confianza de su víctima y hacerla sentir que es su apoyo y así poderle robar información.

**4.2.1.8** ***Quid Pro Quo*****.** Consiste en que el atacante promete algún beneficio a la víctima a cambio de la entrega de información sensible de una empresa o personal.

**4.2.1.9** **Redes sociales y uso de ingeniería social.** Son plataformas en internet con espacios diseñados para que una persona publique, comparta e interactúe con un grupo de personas. Entre la información que se puede compartir está información personal, profesional con terceros e internautas[38]. Más allá de las definiciones puntuales, de lo que semánticamente represente una red social, lo cierto del caso es que ha sido un espacio creado virtualmente para facilitar la interacción entre personas. Desde luego, esta interacción está marcada por algunos aspectos particulares como el anonimato total o parcial, si así el usuario lo deseara, la facilidad de contacto sincrónico o anacrónico, así como también la seguridad e inseguridad que dan las relaciones que se suscitan por esta vía. Las redes sociales son el sitio perfecto para realizar trabajo de campo en busca de información de posibles víctimas, para obtener los mejores resultados se desarrollan basándose en los siguientes puntos[39]. Este proceso se ha especializado y al momento de ejecutar ataques de ingeniería social a través de redes sociales se pueden destacar algunos pasos entre los que se encuentran:

- **Paso 1.** Recolección de información en redes sociales, para ello el delincuente se registra con datos falsos.
- **Paso 2.** Consolidan un plan de ataque para transmitir fiabilidad.
- **Paso 3.** Recolectan información particular, entienden su comportamiento (temas

[38] HÜTT HERRERA, Harold. Las redes sociales: Una nueva herramienta de difusión. En: Redalyc: Revista Reflexiones [en línea]. Costa Rica: Universidad de Costa Rica, enero-junio de 2011. vol. 91, nro. 2. p. 121-128. [Consultado: 23 de septiembre de 2020]. Disponible en https://www.redalyc.org/pdf/729/72923962008.pdf. E-ISSN: 1021-1209.
[39] ROMERO RUBIO, Op. cit., p.3.

de interés, amigos, gustos, etc.), y ganan su confianza.

- **Paso 4.** El atacante hace su primer acercamiento (con un falso perfil) teniendo ya definida la táctica de engaño que va a utilizar.
- **Paso 5.** Cuando la víctima lo considera “su amigo,” el delincuente se muestra cercano y siempre intentará sonsacarle aún más información a través de mentiras.
- **Paso 6.** Una vez se hace “amigo,” el ciberdelincuente pedirá datos más personales (correo electrónico, dirección, número de teléfono, etc.).
- **Paso 7.** En este punto, la identidad podría suplantar de una manera más rápida y eficiente, o se le enviaría a través de correo electrónico un enlace llamativo que al abrirlo ejecutase un troyano que infecta el computador y diera acceso a las cuentas bancarias de la víctima.
- **Paso 8.** Después de obtener lo que buscaba el atacante borra todo rastro, abandona perfiles y no vuelve a hablar con la víctima.

**4.2.1.10 Ejecución de ataques de Ingeniería social.** La ingeniería social en correos electrónicos y redes sociales, es el complemento para los atacantes ya que para la fase de reconocimiento de sus víctimas en las redes sociales pueden encontrar infinidad de información entre los que se encuentran datos personales, sitios, gustos correos, números telefónicos, grupo social etc. misma que los atacantes podrán usar para llegar a su víctima, pasada la etapa inicial cobra importancia el correo electrónico porque es el medio no presencial que permite presionar al usuario a realizar diferentes acciones sustentadas en el engaño, para ello se suplantan sitios oficiales de empresas donde los cuerpos del mensaje incluyen *links* con acceso a páginas clonadas y por medio de *phishing* se recopila información adicional, entre los que se encuentran datos bancarios o contraseñas de acceso a plataformas etc.

En ese orden de ideas existe una técnica avanzada de ingeniería social que es el ataque ATP (Amenaza persistente avanzada) proceso con objetivos concretos de ataques enfocados a empresa determinada y que requiere alto grado de cobertura y un periodo de tiempo largo, durante el cual se emplean elaboradas técnicas y uso de *software*

malicioso el cual aprovecha las vulnerabilidades de un sistema informático. Este tipo de ataques se dio a conocer al mundo luego del informe de la empresa *Mandiant*[40] en donde se especificaba como algunos gobiernos lo usaban para tomar ventaja debido a que por medio del espionaje podían conocer las actividades y tecnologías que están manejando otros gobiernos, algunos casos registrados de ataques APT son Operación Aurora (ataque a multinacionales en 2009), Operación *GhostNet* (Espiar a *Dalai Lama* en 2009), Operación *Stuxnet* (Ataque infraestructura SCADA de Irán, Indonesia, India y Estados Unidos en 2010), Operación *Night Dragon* (Ataque multinacionales petroleras, químicas y energía en 2010), Operación *Shady RAT* (Ataque a Naciones Unidas, gobierno y otras empresas en 2011), Operación Nitro ( Ataque a la industria química y defensa para robo de patentes, formulas y procesos de fabricación en 2011) y Operación *Flame* (Ataque países medio oriente en 2012).

De otro lado hay que destacar que este proceso cuenta con un control y monitorización externa que permite la extracción de datos de forma continua. Entre el público objetivo se encuentran:

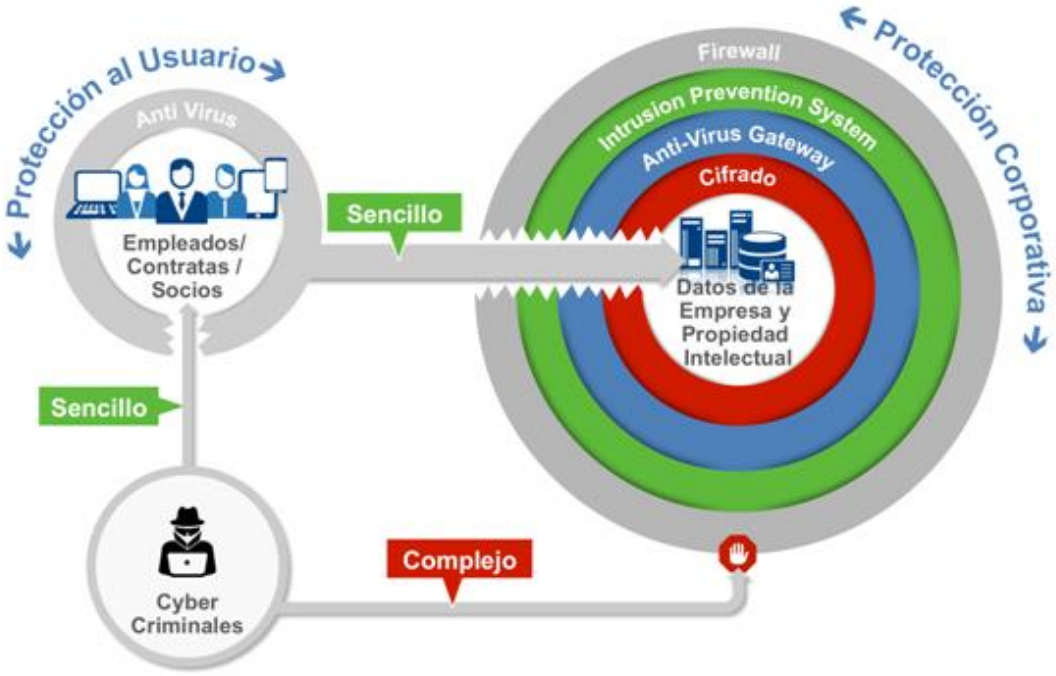
- Sistemas informáticos internos y externos.
- Bases de datos en uso.
- Sistemas de seguridad de la red.
- Sistemas de seguridad del puesto de trabajo.
- Socios conocidos.
- Contratos con terceros.
- Directivos.
- Empleados.

A su vez esta técnica de acuerdo con lo descrito por CEFRIEL ocurre en primer lugar

[40] GOBIERNO DE ESPAÑA, INCIBE. Detección de APTs [sitio web]. España; [Consultado: 07 de mayo de 2021]. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf

cuando el atacante explora y consulta información pública en buscadores web e internet o sin los respectivos filtros de seguridad en redes sociales como *Facebook* o *LinkedIn*, segundo se hace un enfoque o selección del público objetivo, posteriormente se procede con el envío del mensaje con el contenido de ataque, tercero se realiza el envío del mensaje a través de correo electrónico. Lo que sigue luego obedece al éxito o no del ataque, donde si es positiva la respuesta se continúa con la expansión del ataque y la obtención de la información financiera o sensible[41] tal como se muestra en la **Figura 6**.

**Figura 6. Proceso de ataque ATP**




Fuente: https://ibm.co/3ynP1VU

[41] MARIN JIMENEZ, Rafael. Estudio de metodologías de ingeniería social [en línea]. Trabajo de grado Master Interuniversitario en seguridad de las tecnologías de la información y las comunicaciones. Barcelona. *Universitat Oberta de Catalunya* (UOC). Facultad de Informática, Multimedia y Telecomunicación. Departamento de informática, 2018. 133 p. [Consultado: 26 de septiembre de 2020]. Disponible en: Repositorio Educativo Digital UOC. http://hdl.handle.net/10609/81271

## 4.3 MARCO LEGAL

En este espacio se hace la descripción desde lo general a lo particular de algunas normas y leyes creadas por el gobierno para regular el uso de internet, las plataformas tecnológicas y la responsabilidad de los usuarios, mismas que permitan la armonía entre los internautas, es importante conocer los avances o leyes que controlan los delitos informáticos en primer momento y luego llegar a lo particular donde se hace enfoque en las regulaciones para la seguridad informática para verificar si existe regulación centrada en individualizar crímenes cibernéticos principalmente aquellos ataques que usan correos electrónicos y redes sociales para atacar por *phishing*, *malware*, ingeniería social entre otros en áreas como la financiera o entidades gubernamentales colombianas.

En primer lugar, es importante manifestar que desde los diferentes gobiernos existen a nivel legislativo y judicial normas y leyes para proteger los datos de las personas y mejorar la dinámica de las personas y/o empresas en el intercambio de información a través de internet, algunas más ajustadas a la actualidad y los nuevos delitos que otras. En España la ley orgánica 15/1999 estipula que el tratamiento de los datos está encaminado a proteger las transacciones realizadas desde la recopilación, las operaciones y técnicas de limpieza y filtrado, envío de comunicaciones hasta la supresión final de la información[42]. De igual manera en Colombia existen leyes para protección de datos o ley 1581 de 2012 que contempla algo similar a la de España y además es clara en citar que la persona es la dueña absoluta de sus datos personales y que para dar manejo a su información es necesario que este sea notificado y además conozca cual es el fin especifico y sea el usuario quién decida si otorga o no el uso. Se puede notar que desde el gobierno colombiano se brindan garantías a empresas y personas para proteger sus datos a través de la Ley protección de datos, mecanismo legal por medio del cual se reconoce y protege el derecho que tienen las personas a conocer actualizar y rectificar

[42] MIGUEL PEREZ, Julio Cesar. Protección de datos y seguridad de la información [en línea]. 4 ed. Madrid: RA-MA. 2015, 271 p. [Consultado el 26 de septiembre de 2020]. Disponible en: Base de datos libros Google. https://books.google.com.co/books?id=To6fDwAAQBAJ&lpg=PA1&hl=es&pg=PA1#v=onepage&q&f=false ISBN 978-84-9964-560-5.

las informaciones que se hayan recogido sobre ellas en bases de datos o archivos que sean susceptibles de tratamiento por entidades de naturaleza pública o privada[43]

Como se puede evidenciar en los casos anteriores existen diferentes regulaciones y normatividades vigentes las cuales son indispensables para la sana convivencia de las personas, pero además las personas juegan un papel fundamental para proteger y salvaguardar su información, ya que si esta no protege su confidencialidad. no es cautelosa y no se encuentra constantemente capacitada por su desconocimiento o imprudencia corre el riesgo de ser extorsionada y ser expuesta su privacidad.

Pero de la misma forma como hay derecho a rectificar y decidir sobre la información personal, también hay deberes para un uso responsable de los servicios informáticos y respetar los derechos de los demás, en la Ley 1273, quién da las herramientas legales para combatir estos delitos. Cabe destacar que para lograr que para ampliar el alcance legal por medio de la Ley 1273 de 2009 se modificó el Código Penal y se incluyeron penas para delitos digitales como el acceso abusivo a sistemas informáticos, la interceptación de datos informáticos, la violación de datos personales o el uso de *software* malicioso, entre otras conductas[44]. Y también en referencia a los datos la ley 1266 de 2008 se crea para dar claridad y tener una demarcación puntual en lo referente a datos personales es así como esta ley la define como cualquier información que provenga de una o más personas bien sean naturales o jurídicas determinadas o determinables. Además de estas leyes, se creó un sistema de monitoreo y atención de incidentes relacionados con ciberataques, los cuales se manejan desde un centro de ciberataques de la policía nacional colombiana.

En efecto se puede evidenciar que en Colombia existen avances en el tema de

[43] SUPERINTENDECIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales [sitio web]. Bogotá; [Consultado: 28 de septiembre de 2020]. Disponible en: https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

[44] CONGRESO DE LA REPÚBLICA DE COLOMBIA, SENADO. Ley 1273 de 2009 [sitio web]. Bogotá; [Consultado: 28 de septiembre de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

legislaciones contra los delitos informativos, por ejemplo, a nivel de *phishing* y redes sociales las sanciones se realizan con base a la ley 1273 de 2009 la cual tiene dos capítulos tras la adición realizada al código penal del título VII BIS y que tiene que ver con la protección de la información y los datos **Tabla 2 y Tabla 3**. Es así como a partir de lo anterior se podrían configurar dos categorías de delitos, el primero concerniente a la confidencialidad, la integridad, y la disponibilidad de los datos y sistemas informáticos, y el segundo referente a atentados informáticos y otras infracciones.

**Tabla 2. Ley 1273 de 2009 delitos informáticos en Colombia Capitulo 1**

| Capítulo 1 | Delito | Sanción |
|---|---|---|
| Artículo 269A | Acceso abusivo a sistema informático | Prisión de 48 – 96 meses y multa de 100 – 1000 SMMLV para accesos por fuera de lo acordado o no autorizados por el dueño a parte o a todo el sistema informático este protegido o no. |
| Artículo 269B | Obstaculización ilegitima de sistema informático o red de telecomunicaciones | Prisión de 48 – 96 meses y multa de 100 – 1000 SMMLV para quién obstaculice o impida el acceso o funcionamiento normal de sistema, la red y a los datos que estos contienen y lo haga sin estar facultado o autorizado. Si existe una pena mayor se aplica la más alta. |
| Artículo 269C | Interceptación de datos informáticos | Prisión de 36 – 72 meses para quién intercepte datos en el interior o destino de un sistema informático o use emisiones magnéticas para para captura datos sin estar autorizado por orden judicial. |
| Artículo 269C | Interceptación de datos informáticos | Prisión de 36 – 72 meses para quién intercepte datos en el interior o destino de un sistema informático o use emisiones magnéticas para para captura datos sin estar autorizado por orden judicial. |
| Artículo 269D | Daño informático | Prisión de 48 – 96 meses y multa de 100 – 1000 SMMLV para quién borre, altere, dañe, destruya, suprima o deteriore datos o sistemas de tratamiento de estos, o medios de almacenamiento que los contengan sin estar facultado o autorizado. |
| Artículo 269E | Uso de *software* malicioso | Prisión de 48 – 96 meses y multa de 100 – 1000 SMMLV para quién produzca, adquiera, trafique, distribuya, venda, envíe, extraiga o introduzca del territorio nacional software malicioso o dañino. |

Fuente: Propia, adaptado de https://bit.ly/3h7QbPx

**Tabla 2. (Continuación)**

| Capítulo 1 | Delito | Sanción |
|---|---|---|
| Artículo 269G | Suplantación de sitios web para capturar datos personales | Prisión de 48 – 96 meses y multa de 100 – 1000 SMMLV para quién use *phishing* y/o diseñe, desarrolle, trafique, venda, ejecute, programe, o envíe páginas web, enlaces o ventanas emergentes en redes sociales, mensajería, redes sociales entre otros sin estar facultado o autorizado. Si existe una pena mayor se aplica la más alta. |
| Artículo 269H | Circunstancias de agravación de penas | Se incrementan las penas de la mitad a las tres cuartas partes en estos casos:<br>• Ataques a redes o sistemas informáticos o telecomunicaciones del sector oficial/gubernamental, financiero nacionales o extranjeros.<br>• Ataques provenientes de un servidor público activo.<br>• Abuso de confianza contra el tenedor o vinculo de la fuente de información.<br>• Revelar información que perjudique al dueño de esta.<br>• Usar datos para obtener beneficios propios o para un tercero.<br>• Uso con fines de terrorismo o para poner en riesgo la seguridad de país.<br>• Utilización de terceros de buena fe como instrumentos para demostrar confianza.<br>• Aprovechamiento de posiciones de administración o manejo de información. Adicionalmente se inhabilitará profesionalmente para el ejercicio en sistemas de información digital hasta por tres años |

Fuente: Propia, adaptado de https://bit.ly/3h7QbPx

**Tabla 3. Ley 1273 de 2009 delitos informáticos en Colombia Capitulo 2**

| Capítulo 2 | Delito | Sanción |
|---|---|---|
| Artículo 269I | Hurto por medios informáticos y similares | Prisión de 36 – 96 meses para quién manipule un sistema de seguridad informático, telemático o similar, o acceda a la red de telecomunicaciones o suplante usuarios para autenticarse y extraer información sin autorización. Si la cuantía es mayor a 200 SMMLV la sanción será incrementada en la mitad. |
| Artículo 269J | Transferencia no consentida de activos | Prisión de 48 – 120 meses para quién fabrique, posea, facilite y manipule un sistema de seguridad informático o similar, también que realice transferencia de activos afectando a terceros o acceda a la red de telecomunicaciones o suplante usuarios para autenticarse y extraer información sin autorización para cometer delitos o estafas. Si existe una pena mayor se aplica la más alta. Si la cuantía es mayor a 200 SMMLV la sanción será incrementada en la mitad. |

Fuente: Propia, adaptado de https://bit.ly/3h7QbPx

En lo que se refiere a *phishing* es el articulo 269G de la ley 1273 el que castiga este tipo de conductas provengan de cualquier medio (correo electrónico, mensajería, redes sociales, entre otros.) cuyos castigos son prisión de 48 a 96 meses y multa de 100 a 1000 SMMLV si no existe una pena incurrida de mayor gravedad y además la pena puede incrementarse cuando el atacante use varias víctimas dentro del delito aumentan. Por otro lado, el código penal de la 1273 (artículo 58) castiga todo delito que utilice un medio informático, electrónico o telemático.

# 5. METODOLOGIA

Este documento se encuentra dividido en las siguientes fases:

**Fase 1:** En la fase uno se realiza la revisión bibliográfica de los casos de ataques de ingeniería social en correos electrónicos y redes sociales para consolidación de amenazas en el sector financiero y entidades gubernamentales colombianas entre los años 2015 y 2020 por medio de la consulta de documentos académicos, científicos e informes corporativos.

**Fase 2:** En la fase dos se presentan las tendencias y patrones de comportamiento de los ataques ocurridos entre los años 2015 y 2020 de las técnicas y metodologías de Ingeniería social utilizadas en correos electrónicos y redes sociales de empresas del sector financiero y entidades gubernamentales colombianas para lo cual se hace uso de tablas y gráficos los cuales están alineados con base a *OWASP top* 10 documento que recopila los riesgos de seguridad más importantes.

**Fase 3:** La fase tres se muestran las principales vulnerabilidades y amenazas que explotan los ataques de ingeniería social para las empresas objeto de estudio para esto se hace uso de tablas y gráficos los cuales están alineados con base a *OWASP top* 10.

**Fase 4:** se hace una serie de recomendaciones con base a las principales técnicas, metodologías, vulnerabilidades y amenazas de Ingeniería social en correos electrónicos y redes sociales de empresas del sector financiero y entidades gubernamentales colombianas.

# 6. DESARROLLO DE LOS OBJETIVOS

Teniendo en cuenta que el objetivo principal de este proyecto es analizar técnicas y metodologías de Ingeniería social en correos electrónicos y redes sociales a partir de la revisión bibliográfica que permitan la visualización del estado actual de este tipo de ataques en las empresas del sector financiero y entidades gubernamentales colombianas entre los años 2015 y 2020 a continuación se desarrollan los objetivos específicos que permiten llegar a la solución.

## 6.1 EXAMINAR INFORMACIÓN BIBLIOGRÁFICA DE LAS EMPRESAS DEL SECTOR FINANCIERO Y ENTIDADES GUBERNAMENTALES COLOMBIANAS CON CASOS DE ATAQUES DE INGENIERÍA SOCIAL EN CORREOS ELECTRÓNICOS Y REDES SOCIALES PARA CONSOLIDACIÓN DE AMENAZAS ENTRE LOS AÑOS 2015 Y 2020

En este subcapítulo se procede a examinar información bibliográfica de investigaciones a ataques de ingeniería social, registros del centro de ciberataques ocurridos entre los años 2015 y 2020 en las empresas del sector financiero y entidades gubernamentales colombianas utilizando como canal de comunicación correos electrónicos y redes sociales de empleados y/o la misma empresa apoyados en el camuflaje o suplantación de empresas populares o conocidas. A partir de lo cual posteriormente se procede a categorizar y consolidar las amenazas de acuerdo con *OWASP top* 10.

Para entrar en contexto es importante hacer una descripción general de cibercrímenes en Colombia, para el 2020 los ciberataques muestran uno de los mayores crecimientos frente a otros años, esto debido al confinamiento obligatorio provocado a causa de la pandemia de COVID 19, para este año el centro de cibercrímenes de Colombia a través del CAI virtual reporta que los ciberdelitos aumentaron 37% comparado con 2019. De otro lado en el año inmediatamente anterior también hubo crecimiento significativo

aunque más moderado y no tan alto como el de 2020, en consecuencia el informe del 2019 sobre Cibercrimen en Colombia de la Policía Nacional Colombiana[45] reporta que hay 17531 casos de ataques informáticos, notándose un incremento respecto al 2018 del 54% de acuerdo con la **Tabla 4**, donde los mayores casos se generaron en Bogotá (5308), Cali (1190), Medellín (1186), Barranquilla (643) y Bucaramanga (397) donde los principales delitos son hurto de medios electrónicos con un total de 31058 casos, de los cuales los delincuentes buscan extraer dinero de cuentas bancarias; Violación de datos personales con 8037 casos, cuyo objetivo es el robo de identidad para empresas y personas; acceso abusivo al sistema informático con 7994 casos que buscan comprometer sistemas informáticos a través del acceso por ingeniería social; transferencia no consentida de activos con 3425 casos, encaminada a extraer dinero o transferir activos financieros de las víctimas; finalmente se encuentra el uso de *software* malicioso con 2387 casos[46].

**Tabla 4. Comportamiento de delitos informáticos en Colombia**

| Año | Casos registrados |
|---|---|
| 2015 | 7.523 |
| 2016 | 11.225 |
| 2017 | 15.480 |
| 2018 | 22.524 |
| 2019 | 17.531 |
| 2020 | 32.000 |

Fuente: https://bit.ly/35Wc3qo

Ahora bien, a nivel de empresas también se ha notado un crecimiento de los delitos informáticos en ciertos periodos de tiempo, uno de ellos es el comprendido entre el 2015 y 2016 donde el incremento fue de un 5% al 28% de acuerdo con Giraldo y la investigación realizada en el 2018, según él se debe a falta de políticas claras las cuales

[45] POLICÍA NACIONAL DE COLOMBIA, CAI VIRTUAL, Op. cit., p.2.
[46] Ibid., p.2

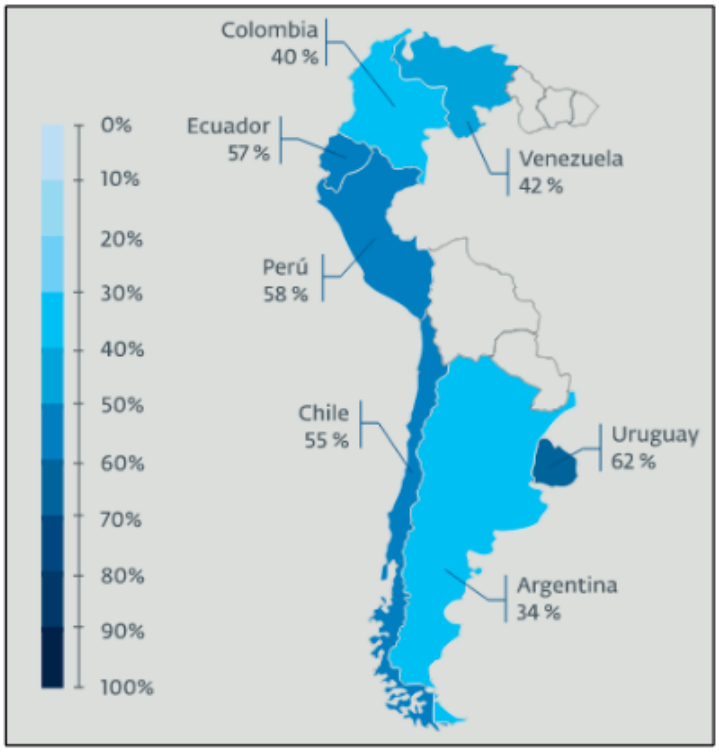
hacen que se lleven a cabo malas prácticas en el uso de los sistemas informáticos y de red[47]. Se debe tener en cuenta que el acceso desde casi cualquier lugar y dispositivo a través de internet generan riesgos que las soluciones tradicionales de seguridad y gestión del riesgo sean ineficaces para controlar y/o detectar. De conformidad con lo anterior es muy importante promover desde el gobierno y las empresas en conjunto campañas, normas y estándares que permitan a las empresas apropiarse sobre el uso de buenas prácticas de seguridad informática y la información, teniendo presente que es de gran importancia la capacitación constante a sus trabajadores sobre ataques de ingeniería social y nuevas políticas de seguridad acordes a la nueva forma de comunicación y hacer las cosas, es así como las empresas deben adoptar controles a nivel de la infraestructura y talento humano y establecerlo como una política al interior de su plan de funcionamiento.

De acuerdo con la **Figura 7** el autor muestra como para Colombia hubo accesos ilegales a las bases de datos, lo cual es motivo de preocupación y alerta a las empresas sobre el cuidado para tener en cuenta para fortalecer la seguridad de la información y así garantizar la confidencialidad, integridad y disponibilidad de la información. Además, estos ataques de ingeniería social impactan negativamente en el *core* del negocio viéndose afectados principalmente en lo referente a la reputación, disrupción de los procesos misionales e insatisfacción del cliente, todo esto finalmente impacta negativamente a nivel de la economía y afecta seriamente la huella digital que realizan las empresas debido a su presencia en internet para ejercer muchas de sus actividades diarias (Reputación y presencia *online*). La transformación digital está cambiando el mundo y las empresas más rápido que nunca han tenido que migrar a este nuevo escenario “el internet” y consigo hay nuevos retos que enfrentar, existen nuevos tipos de

[47] GIRALDO MARTINEZ, Jenny Paola y PACHECO DUARTE, Iván Guillermo. Ingeniera social: técnica de ataque *phishing* y su impacto en las empresas colombianas [en línea]. Trabajo de grado especialización en seguridad informática. Salamina. Universidad Nacional Abierta y a Distancia - UNAD. Facultad de ingeniería y ciencias básicas. Departamento de sistemas, 2018. 90 p. [Consultado: 10 de noviembre de 2020]. Disponible en: Repositorio Educativo Digital UNAD. https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/27050/1/jpgiraldoma.pdf

amenazas provenientes de los ciberdelincuentes que también encontraron a este escenario el propicio para generar nuevas formas de lucrarse y hacer daño a las empresas, principalmente entidades de gobierno y banca, hay nuevas formas de explotar vulnerabilidades que actualmente están generando nuevos riesgos para el core del negocio de las empresas.

**Figura 7. Reporte de accesos indebidos a bases de datos y *software* a empresas en latinoamerica.**



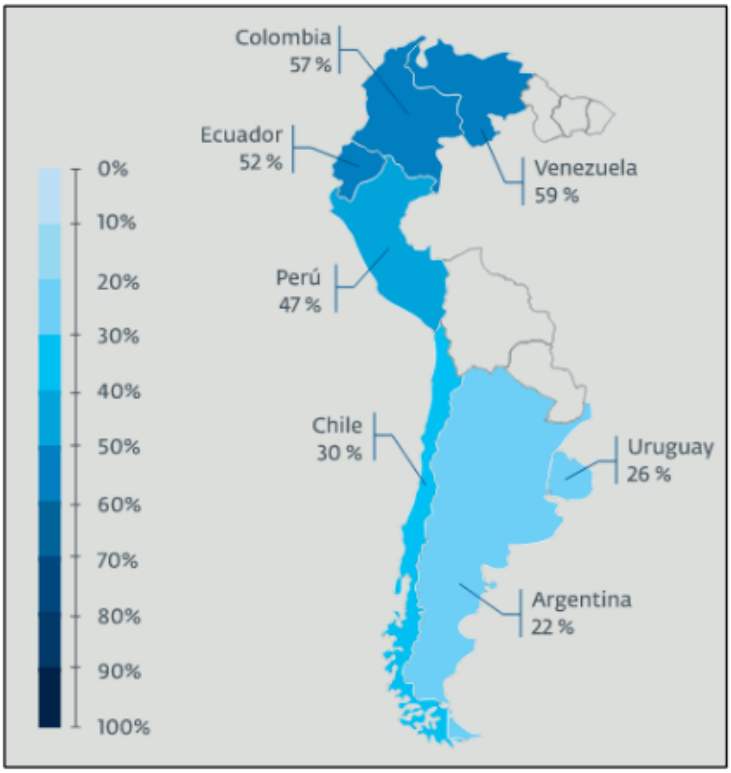

Fuente: https://bit.ly/3zUPVum

Asimismo, ESET[48] en el 2015 realiza un análisis de los ataques informáticos en Latinoamérica basados en el desarrollo de una encuesta a las empresas, en donde se pudo obtener datos importantes sobre el tipo de ataques perpetrados, para el caso de

[48] ESET; Security report; Latinoamérica 2015; [sitio web]. Latinoamérica: ESET. [Consultado: 20 de mayo de 2021]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf

Colombia se encontraron que los ataques por *phishing* ocurrieron en un 57% de los ataques por *malware* tal como se muestra en la **Figura 8**. Lo anterior demuestra como a la fecha continúan en furor los ataques de *malware* tipo *phishing* quizás debido al rápido uso de las plataformas digitales y transición que la mayoría de las empresas están realizando en pro de generar nuevas formas de comunicarse y la apertura de nuevos mercados a través de internet y que es explotada por ciberdelincuentes. De allí que se requiere del fortalecimiento y la planificación desde un escenario centrado en la seguridad de la información y los sistemas de gestión de seguridad de la información (SGSI) de las organizaciones, aportando a la empresa de una forma integral teniendo en cuenta la infraestructura, las herramientas informáticas y empleados y/o personas conocedoras del tema. Lo anterior conllevara a disminuir el riesgo de ataques a los activos de información de las empresas y generar entornos seguros.

**Figura 8.Comportamiento de ataques a empresas en Latinoamérica.**




Fuente: https://bit.ly/3zUPVum

Ahora bien, como marco de referencia en la clasificación del grado de riesgo de las amenazas y el impacto en la seguridad de la información en las entidades objeto de este documento se utilizará el estándar *OWASP top* 10 que se muestra en la **Figura 9** el cual es un organismo sin ánimo de lucro cuyo nombre proviene del inglés y traduce proyecto abierto de seguridad de aplicaciones web (*OWASP*) y está formada por empresas, sector educativo y particulares a nivel mundial que proporcionan información útil, veraz e imparcial y que tiene como propósito investigar, analizar, determinar y combatir los diez riesgos más importantes en entornos web, para que así las empresas o administradores informáticos conozcan las causas que hacen a un *software* inseguro y puedan combatir o alertarse frente a las vulnerabilidades explotadas por los ciberdelincuentes.

**Figura 9. Evolución de amenazas de acuerdo con las técnicas de ataque en los últimos diez años.**

| OWAPS TOP 10 - 2007 | | OWAPS TOP 10 - 2010 | | OWAPS TOP 10 - 2013 | | OWAPS TOP 10 - 2017 |
|---|---|---|---|---|---|---|
| A1 – Secuencia de Comandos en Sitios Cruzados (XSS) | ▲ 1 | A1 – Inyección | = 0 | A1 – Inyección | = 0 | A1 – Inyección |
| A2 – Inyección | ▼ -1 | A2 – Secuencia de Comandos en Sitios Cruzados (XSS) | ▲ 1 | A2 – Pérdida de Autenticación y Gestión de Sesiones | = 0 | A2 – Pérdida de Autenticación |
| A3 – Ejecución Maliciosa de Ficheros | ⇧ 4 | A3 – Pérdida de Autenticación y Gestión de Sesiones | ▼ -1 | A3 – Secuencia de Comandos en Sitios Cruzados (XSS) | ⇧ 3 | A3 – Exposición de Datos Sensibles |
| A4 – Referencia Directa Insegura a Objetos | ▲ 1 | A4 – Referencia Directa Insegura a Objetos | = 0 | A4 – Referencia Directa Insegura a Objetos | (*) | A4 - XML External Entities (XEE) |
| A5 – Falsificación de Peticiones en Sitios Cruzados (CSRF) | = 0 | A5 – Falsificación de Peticiones en Sitios Cruzados (CSRF) | ▲ 1 | A5 – Configuración de Seguridad Incorrecta | (**) | A5 - Perdida de Control de Acceso |
| A6 – Filtrado de Información y Manejo Inapropiado de Errores | (*) | A6 – Defectuosa Configuración de Seguridad | (*) | A6 – Exposición de Datos Sensibles | ▼ -1 | A6 – Configuración de Seguridad Incorrecta |
| A7 – Pérdida de Autenticación y Gestión de Sesiones | ▲ 1 | A7 – Almacenamiento Criptográfico Inseguro | (*) | A7 – Ausencia de Control de Acceso a las Funciones | ⇩ -4 | A7 – Secuencia de Comandos en Sitios Cruzados (XSS) |
| A8 – Almacenamiento Criptográfico Inseguro | ▲ 2 | A8 – Falla de Restricción de Acceso a URL | ⇩ -3 | A8 – Falsificación de Peticiones en Sitios Cruzados (CSRF) | (*) | A8 - Deserialización insegura |
| A9 – Comunicaciones Inseguras | (*) | A9 – Protección Insuficiente en la Capa de Transporte | (*) | A9 – Uso de Componentes con Vulnerabilidades Conocidas | = 0 | A9 – Uso de Componentes con Vulnerabilidades Conocidas |
| A10 – Falla de Restricción de Acceso a URL | (*) | A10 – Redirecciones y reenvíos no validados | = 0 | A10 – Redirecciones y reenvíos no validados | (*) | A10 - Registro y monitorización insuficiente |
| (*) Nuevo (**) Fusionado | | | | | | |

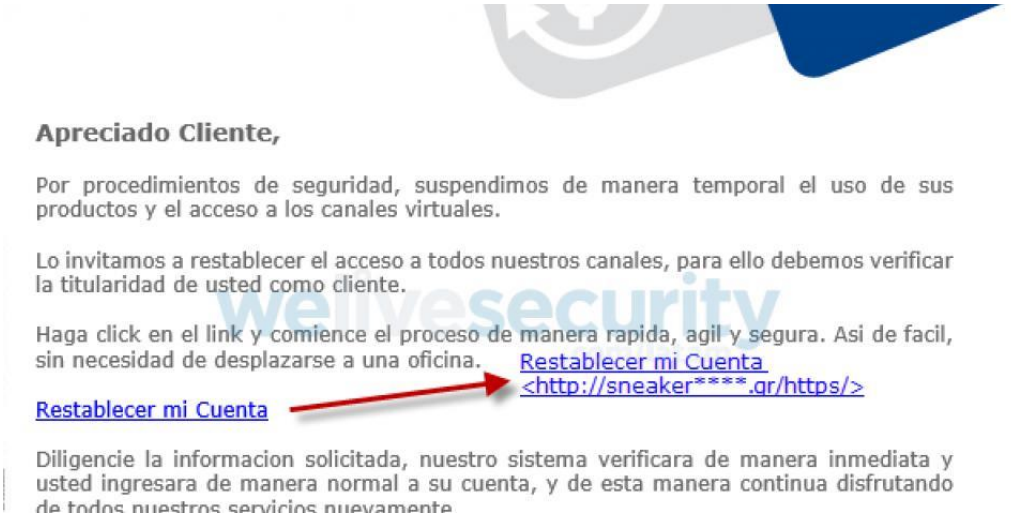
Fuente: https://bit.ly/3hdGP3u

A continuación, se realiza una verificación de los casos de ataques y se procede a categorizar las diferentes amenazas encontradas y ver cuales impactan en los sectores bancario y gubernamental.

### 6.1.1 Ingeniería social en sector Bancario

Actualmente existe muy poca documentación de ciberataques a entidades bancarias, principalmente por temas de seguridad y reputación de estas. Un caso documentado es el del año 2017 del ataque de *phishing* a Bancolombia, uno de los bancos con más usuarios en el país colombiano. De acuerdo con las declaraciones de ESET el fraude se originó mediante un correo electrónico información@bancolombia.com.co donde se le notificaba sus usuarios que por seguridad los servicios que tenían con este banco habían sido suspendidos temporalmente por motivos de seguridad y que por tal razón se debía actualizar datos mediante un enlace proporcionado en el correo, el cual solicitaba contraseña, usuario y demás información del titular de la cuenta tal como se observa en la **Figura 10**. Una vez obtenían los datos este ataque tenía como fin sustraer dinero de las cuentas mediante transferencias, describe el autor que incluso los atacantes diseñaron una interfaz muy similar a la del banco, incluyendo el teclado virtual para ingreso de contraseña[49].

**Figura 10. Correo electrónico *phishing* suplantando a Bancolombia.**




Fuente: https://repository.unad.edu.co/handle/10596/18701

[49] PEREZ, Yolman. Un caso de phishing más en Colombia [en línea]. Sala de conocimiento Universidad Cooperativa de Colombia. Arauca. (25 de abril de 2017). [Consultado: 15 de noviembre de 2020]. Disponible en: https://www.ucc.edu.co/prensa/2016/Paginas/un-caso-de-phishing-mas-en-colombia.aspx

Para combatir estos delitos es importante documentarse constantemente a través de los diferentes consejos que emiten las páginas oficiales de los bancos y el gobierno. Ante todo, se debe mantener el beneficio a la duda y si la persona no tiene conocimiento del tema es mejor abstenerse de usar medios digitales. Con esto no se busca fomentar el miedo, pero si generar conciencia en las personas para que se capaciten, duden y a su vez realicen diligencias en internet con responsabilidad, seguridad y terminales conocidas, ya que es el capital de toda su vida de trabajo el que puede estar en riesgo.

Teniendo en cuenta casos como el relacionado de ingeniería social, la pregunta es cómo actúan los bancos y hasta donde tienen que responder por sus clientes ya que un caso de ataques de ingeniería social esta perpetrado por un tercero que aprovecha la ingenuidad de las personas. Frente a esta cuestión el autor muestra dos posturas, la primera responsabilizando al banco y a asumir cualquier reparación de ocurrir algún ataque a los activos del cliente, pues se entiende que cualquier transacción generada por medios electrónicos representa riesgo y el banco debe brindar las condiciones para hacerlo, si se materializa cualquier ataque significaría que los bancos no han tomado las medidas de seguridad necesarias. A su vez la segunda postura está encaminada a eximir al banco de responsabilidades toda vez que un ataque provenga del ataque de un tercero que por medio de artimañas logra engañar o chantajear por medio de ingeniería social, además, se alega la existencia de una relación contractual entre las partes y que las disposiciones que se aceptaron por los clientes son vinculantes[50].

Frente a esta posición y teniendo en cuenta la importancia de proteger la privacidad de las personas es necesario continuar protegiendo al cliente pues el usuario del banco continúa siendo el ente más vulnerable de este esquema de negocio, ahora bien, para ello los bancos deben realizar promoción y prevención de ataques de ingeniería social y fortaleciendo la infraestructura de TI y comunicaciones de acuerdo con ciertos estándares

[50] ZABALA, Jhon Alexander. Responsabilidad bancaria frente al delito de phishing en Colombia [en línea]. Trabajo de grado Pregrado en Derecho. Bogotá. Universidad Católica de Colombia. Facultad de Ciencias Sociales y políticas. Departamento de derecho, 2017. 26 p. [Consultado: 16 de noviembre de 2020]. Disponible en: Repositorio Educativo Digital UCATOLICA. http://hdl.handle.net/10983/14943

de calidad y seguridad de la información, a su vez hacer una amplia difusión por medio de la capacitación y sensibilización de las personas frente a las amenazas y la responsabilidad que se debe tener al momento de realizar transacciones a través de internet, de esta forma se podrá mitigar los ataques y hacer que estos tengan menor efectividad.

Teniendo en cuenta el estándar *OWASP top* 10 se encuentra que el uso de *phishing* en el sector financiero representa una grave amenaza que puede terminar en la exposición de datos sensibles (A3) y pérdida de autenticación y gestión de sesiones (A2) que este corresponde a uno de los problemas más comunes citados en la versión 2017 del estándar mencionado anteriormente. Asimismo, muchos de los ataques de ingeniería social aprovechan configuraciones de seguridad incorrectas (A6) que también es uno de los problemas comunes listados en el estándar *OWASP*.

### 6.1.2 Ingeniería social en entidades Gubernamentales

En el año 2017 se reporta un ataque de *phishing* a la DIAN[51], para ello se utiliza correos falsos y que usan una estructura similar a los oficiales tal como se observa en la **Figura 11**, en donde el correo lleva consigo asuntos como “Hasta la fecha no hemos recibido el pago de tus impuestos”, “Notificación de embargo DIAN” o “Problemas con tu situación fiscal” y uno de los correos más usados se originó mediante el correo electrónico minhacienda@dian.gov. Cabe mencionar que frente a estos hechos la entidad oficial DIAN se pronunció y confirmo que se estaban generando correos suplantados para estafar por parte de terceros e invito a sus usuarios a no caer en este tipo de ataques tipo *phishing* y a su vez recomendó realizar el respectivo reporte y además antes de realizar cualquier acción siempre validar la veracidad de la información recibida y que

[51] PLAZAS GARCIA, Edna Rocio. Ingeniera social: en las empresas colombianas [en línea]. Trabajo de grado especialización en seguridad informática. Pitalito. Universidad Nacional Abierta y a Distancia - UNAD. Facultad de ingeniería y ciencias básicas. Departamento de sistemas, 2018. 75 p. [Consultado: 20 de mayo de 2021]. Disponible en: Repositorio Educativo Digital UNAD. https://repository.unad.edu.co/handle/10596/18704

corresponda a correos oficiales de la institución, ser cautelosos y evitar ingresar datos personales en los enlaces adjuntos de este tipo de correos.

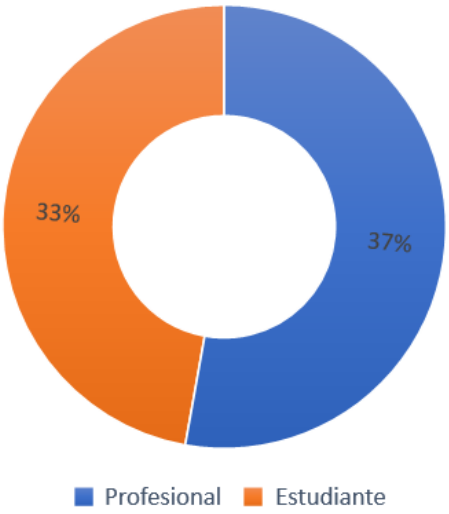
**Figura 11. Estructura de correo fraudulento suplantando a la DIAN.**


Fuente: https://repository.unad.edu.co/handle/10596/18704

De otro lado, como caso típico en el estudio realizado por Estrada, 2020, denominado Prácticas de seguridad de información del Nivel Ejecutivo de la Policía Nacional de Colombia: Escuela de Policía Simón Bolívar (Tuluá, Colombia) se hace un análisis a nivel de la institución donde el resultado de acuerdo con el **Gráfico 1**, muestra que en promedio

los comportamientos y conocimientos sobre seguridad de la información son de nivel medio y, por tanto, el riesgo de verse asociados a ataques de *phishing* son altos, lo cual implica una necesidad de rediseñar programas de capacitación continua y mantener en el pensum académico asignaturas que incluyan unidades referentes a buenas prácticas de seguridad de la información[52].

**Gráfico 1. Porcentaje de desconocimiento del personal de Escuela de Policía Simón Bolívar de Tuluá en ataques de *Phishing*.**




Fuente: Propia, adaptado de https://bit.ly/3xBxHfL

Lo anterior constata el éxito de este tipo de campañas generadas por medio de ataques de ingeniería social y *phishing* en las empresas para estafar utilizando el engaño. Como se ha mencionado a lo largo de este documento, la persona es el eslabón más débil y fácil de utilizar para obtener lo que se requiera a conveniencia. Es así como es de gran importancia invertir en capacitación y actualización constante sobre ataques de ingeniería social a los diferentes grupos de personas que hacen parte de una empresa.

[52] ESTRADA ESPONDA, Royer David. Prácticas de seguridad de información del Nivel Ejecutivo de la Policía Nacional de Colombia en la Escuela de Policía Simón Bolívar (Tuluá, Colombia). En: Ciencia y Tecnología estudio de caso [en línea]. Logos: Policía Nacional de Colombia, enero-abril de 2020, vol. 12, nro. 1. 131 p. [Consultado: 13 de noviembre de 2020]. Disponible en https://revistalogos.policia.edu.co:8443/index.php/rlct/article/view/1050. ISSN 0121-0777.

Resultado similar se encuentra en el estudio de Benavides en el 2020 realizado a un grupo de colaboradores de su confianza, donde a través de la red social *Facebook* y *WhatsApp* se invitó a acceder a un blog personal el cual contiene un código malicioso que realiza la instalación de un *script* a cada uno de los dispositivos personales, el cual puede recolectar información del usuario entre los cuales están la IP, Nacionalidad, sistema operativo, navegador entre otros. Tal como se muestra en la **Figura 12**, para la recolección de datos y motivar a la víctima se hace uso de un contador falso en el blog para dar la sensación de seguridad al mostrar que muchas personas ya ingresaron, a su vez el uso de un código *QR* en el estado de *WhatsApp* busca atraer conocidos y curiosos.

**Figura 12. Recolección de información por medio de Ingeniería social.**


Fuente: https://bit.ly/3xBCiP3

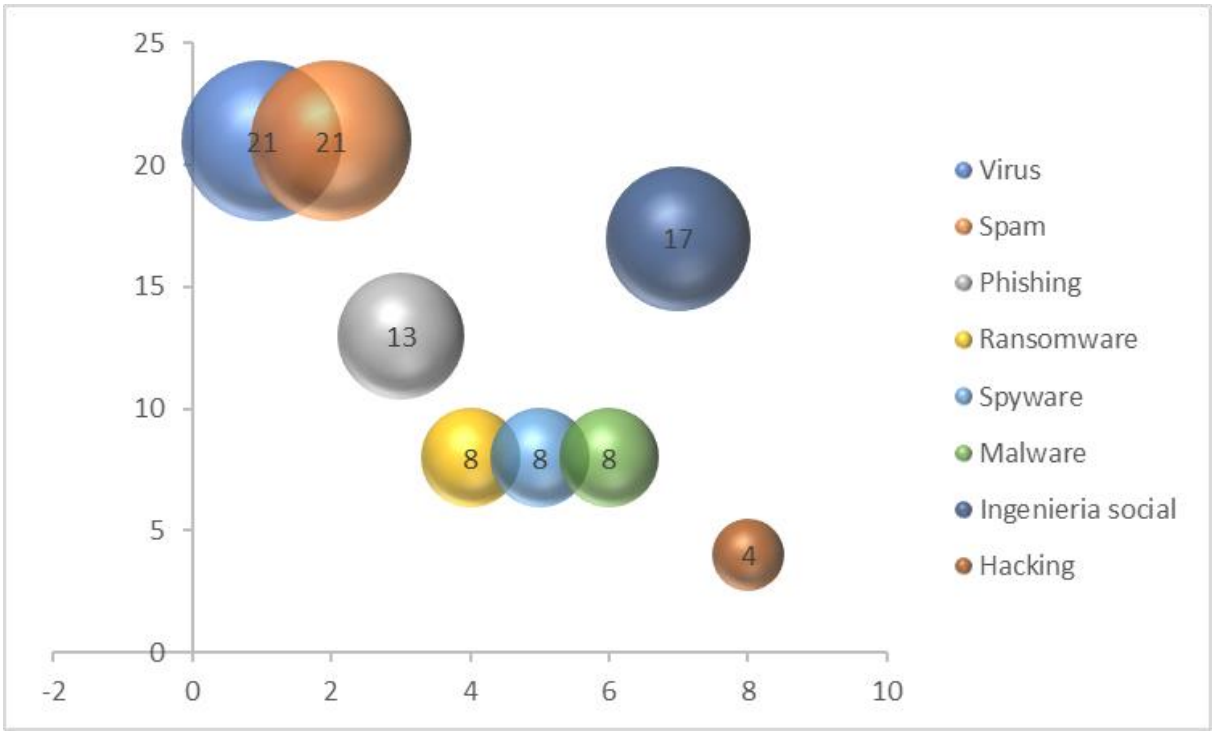
Una vez realizada la recopilación de Información, se crea un ataque para realizar un escaneo del puerto 80 (Servidor web) y puerto 22 (Servidor SSH) en busca de información confidencial. Entre los resultados se observa que muchos equipos se encuentran con las configuraciones por defecto de puertos y además programas y sistemas desactualizados. De igual manera el investigador, para poder contrastar realiza a la par una encuesta sobre conocimiento de ataques de ingeniería social[53], esta le permite conocer la situación de la población encuestada y alertar sobre vulnerabilidades a nivel de usuario, una vez se muestran los resultados, esos sorprenden a los partícipes del experimento ya que por un lado, en la encuesta solo el 2% fue consciente y precavido al momento de entregar datos que le solicitan por medio de un enlace para visitar un blog, los demás entregaron la información sin ningún inconveniente. Por otro lado, los datos que se pudieron sacar por medio del *script* instalado a los dispositivos les inquieto ya que desconocían sobre toda la información que pudieron obtener de ellos, además no eran conscientes que existen muchas vulnerabilidades a nivel de sistema operativo y aplicaciones y que requieren tomarse el tiempo de corregirlas.

Otro estudio realizado por Vega[54] en el 2018 en las alcaldías de Huila Colombia muestra que el 21% de los ataques es por virus informáticos, 21% por correos *spam* o no deseados, 17% ingeniería social, 13% *phishing*, 8% *malware*, 8% spyware, 8% *ransomware* y 4% *hacking* tal como se muestra en la **Figura 13**. Estos virus informáticos son una gran amenaza y mas de una vez los usuarios de una empresa deben solicitar apoyo técnico para poder eliminarlos aunque en la mayoría de los usuarios puede estar capacitado muchas veces no tiene las conductas necesarias y el cuidado necesario para evitar la ejecución o mantener los sistemas de defensa de computadores actualizados.

[53] BENAVIDES ASTUDILLO, Eduardo. Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social. En: Ciencia: Revista UNEMI [en línea]. Milagro: Universidad Estatal de Milagro, enero-abril de 2020. vol. 13, nro. 32. p. 27 - 40. [Consultado: 13 de noviembre de 2020]. Disponible en http://ojs.unemi.edu.ec/index.php/cienciaunemi/article/view/1028/1003. E-ISSN: 2528-7737.

[54] VEGA SÁNCHEZ, Fabio Alexander y SUARÉZ LIZCANO, Wilson. Métodos de ataques y prevención de la ingeniería social en las alcaldías del huila en Colombia [en línea]. Trabajo de grado especialización en seguridad informática. Neiva. Universidad Nacional Abierta y a Distancia - UNAD. Facultad de ingeniería y ciencias básicas. Departamento de sistemas, 2018. 85 p. [Consultado: 13 de julio de 2021]. Disponible en: Repositorio Educativo Digital UNAD. https://repository.unad.edu.co/handle/10596/18701

**Figura 13. Amenazas en alcaldías de Huila Colombia durante el 2018**




Fuente: Propia, adaptado de https://bit.ly/2UBxryN

Ahora bien, con las vulnerabilidades encontradas en los casos anteriormente descritos al realizar una aproximación y comparación frente al estándar *OWASP top* 10 sobre los problemas más comunes citados en la versión 2017, se encuentra que las principales amenazas del uso de técnicas de *phishing* en el sector gubernamental son la exposición de datos sensibles (A3), Inyección (A1) pérdida de autenticación y gestión de sesiones (A2). Asimismo, muchos de los ataques de ingeniería social aprovechan configuraciones de seguridad incorrectas (A6) y uso de componentes con vulnerabilidades conocidas (A10).

## 6.2 COMPILAR TÉCNICAS Y METODOLOGÍAS DE INGENIERÍA SOCIAL EN CORREOS ELECTRÓNICOS Y REDES SOCIALES DE EMPRESAS DEL SECTOR FINANCIERO Y ENTIDADES GUBERNAMENTALES COLOMBIANAS QUE PERMITAN LA VISUALIZACIÓN DE TENDENCIAS Y PATRONES DE COMPORTAMIENTO DE LOS ATAQUES OCURRIDOS ENTRE LOS AÑOS 2015 Y 2020.

Contiene la compilación de técnicas y metodologías de Ingeniería social en correos electrónicos y redes sociales de empresas del sector financiero y entidades gubernamentales colombianas que permitan la visualización de tendencias y patrones de comportamiento de los ataques ocurridos entre los años 2015 y 2020.

Para realizar un abordaje integral de la ciberseguridad este documento está alineado con base a la norma ISO 27001:2013 anexo A, esto permitirá clasificar, comprender, gestionar y reducir los riesgos informáticos de acuerdo con las tendencias o patrones encontrados en cada una de las revisiones bibliográficas. En ese sentido de acuerdo con los ataques cibernéticos descritos en el trabajo de Monsalve[55] se encuentra que dentro de las metodologías apoyadas en ingeniería social que los ciberdelincuentes utilizan más frecuentemente se encuentran:

- ***Spear Phishing*.** En la cual los atacantes se enfocan a un grupo reducido y es por lo que casi nunca afectan a entidades bancarias o redes sociales. Se encuentra que estos ataques son con enfoque especifico a personas o empresas con número reducido de personas y perfiles explícitos, generalmente personas con menor grado de conocimiento técnico de plataformas tecnológicas. En este tipo de ataque se busca llegar a un nivel de personalización mayor por ejemplo con datos de la persona, direcciones conocidas y así aumentar la eficacia ante las victimas que

[55] MONSALVE MENDEZ, Jaime Yesid. Ciberseguridad: Principales amenazas en Colombia (Ingeniera social, *Phishing* y *DDoS*) [en línea]. Trabajo de grado especialización en seguridad informática. Bogotá. Universidad Piloto de Colombia. 2018. 75 p. [Consultado: 20 de mayo de 2021]. Disponible en: Repositorio Educativo Digital. http://repository.unipiloto.edu.co/handle/20.500.12277/4663

respondan al ataque, la cual en cierta medida depende de la optimización que se realice al momento de aplicar ingeniería social y estudio previo de las víctimas.

- ***Whaling*.** Es un tipo de *phishing* enfocado a grandes ejecutivos y personas responsables de la toma de decisiones o que tengan a cargo el manejo financiero y la información de una empresa**.** Este tipo de ataques tiene menor porcentaje de éxito ya que generalmente tienen mayor grado de capacitación y conocimiento por lo cual la forma de llegar a ellos es por medio de algo atractivo como por ejemplo una promoción o lanzamiento de un producto o servicio especial.

- ***Cloning*.** Este ataque consiste en enviar un correo con un archivo adjunto a una víctima seleccionada y que una vez el usuario caiga en la trampa el atacante lo utiliza para crear correos electrónicos similares o reales a los dispuestos por una organización víctima y a su vez con estos enviar información falsificada y hacer parecer que proviene de un remitente original.

- ***Phishing* con geolocalización.** Es una técnica que restringe el acceso en una ubicación geográfica determinada de los sitios que utiliza el atacante para así evitar que su IP se bloqueada o reportada más rápidamente asimismo busca llegar a personas y sitios focalizados.

Aunque comúnmente cuando se escucha hablar sobre los ciberataques y la ciberdelincuencia que vulneran sistemas informáticos, las personas lo asocian con *hackers* muy preparados y con gran capacidad para ejecutar complejos códigos en realidad es que esto en la mayoría de los casos no opera de esta manera y la razón principal es porque si se manejara de esta manera significaría hacer una inversión muy alta de tiempo, recursos humanos y dinero. Es así que La mayoría de los ciberataques están enfocados en atacar personas en un mayor número y con la menor inversión posible. Esto se logra por medio de ataques de ingeniería social.

Es así entonces que a nivel de las técnicas más usadas para obtener información y realizar ataques de ingeniería social son las redes sociales, ya que estas son un medio de obtención de información rápida y efectiva, un medio muy utilizado por los ciberdelincuentes para extraer y obtener información. Entre las diferentes técnicas utilizadas está la publicación de noticias falsas de gran impacto como muertes de personajes importantes, desastres o juegos o cadenas para ganar dinero, las cuales tienen un llamado a la atención muy alto y donde las personas muy probablemente van a cliquear para conocer más, según Vega[56] estos *links* falsos pueden solicitar credenciales de acceso a la red social con lo cual pueden tener toda la información de la víctima y así al momento de realizar un ataque *phishing* por correo u otro medio el grado de éxito va a ser muy alto.

A su vez, como se indicó, desde las redes sociales los ciberdelincuentes contactan a la víctima y tratan de generar confianza hasta obtener sus datos. Es el caso que, por ejemplo, en la investigación realizada a una población de estudiantes de la Universidad del Valle por Flórez, se hace un experimento aplicando ingeniería social a través de redes sociales y se logró mostrar la cantidad de información que es posible recopilar de usuarios desprevenidos o incautos incluso hasta de aquellos que aseguraban se los más listos. Como primer dato se realiza una encuesta para determinar el porcentaje de usuarios que utilizan redes sociales se obtuvo que el 59% de los encuestados maneja redes sociales y todos acceden a las plataformas más de una vez al día. Las redes sociales de mayor uso son *Facebook* e *Instagram*, asimismo los encuestados aducen que su uso está ligado a que este es un escenario donde se brinda muchas posibilidades entre ellas poder interacción social, compartir archivos, jugar, organizar eventos, así como promocionar y vender productos o buscar trabajo.

Por otro lado, al realizar la verificación de cada una de las cuentas de los usuarios se encontró que estos utilizan contraseñas poco seguras, el 55% de los encuestados no

[56] VEGA SÁNCHEZ, Op. cit., p.35

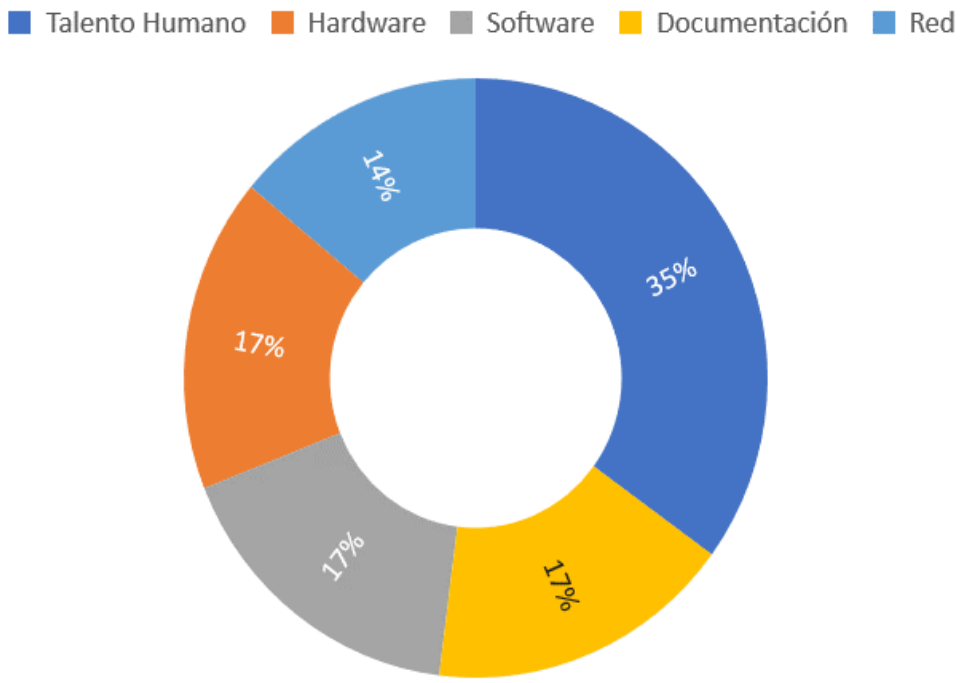
usan claves robustas. Además, se logró identificar que en la universidad no existe un control de acceso a redes sociales, así que los empleados y demás personas pueden acceder a cualquier contenido sin ningún problema. Por otro lado, la mayoría de los empleados no poseen conocimientos fuertes en temas de ingeniería social y ataques *phishing* según lo manifiestan les parece que es algo ajeno a su entorno y que ponerse en la tarea de fortalecer sus contraseñas les complicaría la vida pues difícilmente la recordaran a futuro. Esto demuestra el grado de vulnerabilidad y riesgo al que se enfrentan diferentes compañías por blancos fáciles de atacar, las personas. Un atacante fácilmente podrá aprovechar esta vulnerabilidad y usarla para realizar ingeniería social a través de redes sociales y extraer información para atacarlos y extorsionar [57].

De acuerdo con lo anterior y teniendo en cuenta el **Gráfico 2** se encuentra que dentro de los ataques a los activos de las empresas en los sectores financiero y entidades gubernamentales colombianas, el uso de por ingeniería social al talento humano representa el mayor porcentaje (35%), lo cual concuerda con las precisiones realizadas por Arenas **[58]** respecto el camino más práctico que realiza un ciberdelincuente es a través del abuso de confianza o ingeniería social, el atacante se apalanca del desconocimiento o la ingenuidad de un empleado para acceder a información privada de la empresa, esto permite ganar horas de trabajo y evitar intentos fallidos tras una plataforma informática tratando de acceder a un sistema por la infraestructura de red, proceso que requiere un alto nivel de conocimiento y muchas horas de invasión en estudio.

[57] FLOREZ RAMIREZ, Claudia Patricia y MÉNDEZ COLLO Harold. Estudio de ingeniería social en el uso de las redes sociales [en línea]. Trabajo de grado especialización en seguridad informática. Bogotá. Universidad Nacional Abierta y a Distancia UNAD. Escuela de ciencias básicas, tecnología e ingeniería. Departamento de Ingeniería de Sistemas, 2017. 129 p. [Consultado: 16 de noviembre de 2020]. Disponible en: Repositorio Educativo Digital UNAD. https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14505/1/17659358.pdf

[58] ARENAS BONILLA, Oscar Javier. El eslabón más débil [en línea]. Trabajo de grado especialización en Seguridad Informática. Bogotá. Universidad Piloto de Colombia. Facultad de Ingeniería. Departamento de ingeniería de sistemas, 2016. 8 p. [Consultado: 17 de julio de 2021]. Disponible en: http://polux.unipiloto.edu.co:8080/00001933.pdf

**Gráfico 2. Distribución de activos atacados por ingeniería social**



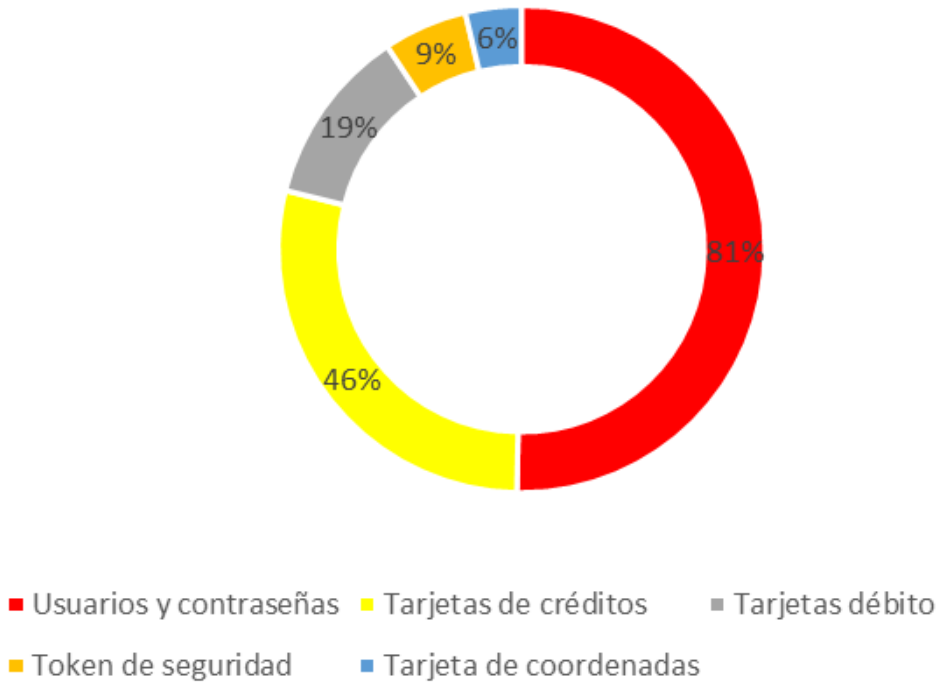

Fuente: Propia, adaptado de https://bit.ly/2UBxryN

Finalmente se puede citar que a nivel de correos electrónicos y redes sociales la técnica más utilizada para robar información es la ingeniería social y el método es más usado es la suplantación de identidad (*phishing*) y que la información de mayor interés por parte de los atacantes corresponde al robo de contraseñas y usuarios (**Gráfico 2**) la cual representa de acuerdo con Pardo, el 81% del total de los ataques *phishing*, por otro lado, los ataques en tarjetas de crédito corresponden al 46% y tarjetas débito con el 19%[59]. Este comportamiento se puede apreciar en la **Figura 14** lo cual visibiliza como cada vez más los delincuentes informáticos van por el control total de un sistema para doblegarlo a su merced y además buscan sustraer el dinero que exista en las cuentas sensible para

[59] PARDO FERRO, Carlos Enrique. Amenazas en la red: entrando al mundo de los ciberataques - ingeniería social, phishing y malware [en línea]. Trabajo de grado especialización en Seguridad Informática. Bogotá. Universidad Piloto de Colombia. Facultad de Ingeniería. Departamento de ingeniería de sistemas, 2018. 12 p. [Consultado: 9 de noviembre de 2020]. Disponible en: Repositorio Educativo Digital UNIPILOTO. http://repository.unipiloto.edu.co/handle/20.500.12277/2647

extraer dinero o atentar contra la confidencialidad de las empresas y personas. Es por lo que cada día las empresas suman esfuerzos en fortalecer sus sistemas, aunque no todos son conscientes de ello, tal como se menciona en otro aparte de este documento. Lo anterior concuerda con lo mencionado por Vega (2018) en su trabajo de investigación donde menciona que los ataques por *phishing* en Colombia son de los más recurrentes y como los ciberdelincuentes utilizan noticias del momento para atraer a las víctimas y lograr que ingresen a enlaces donde les solicitan información privada y datos bancarios[60].

**Figura 14. Información de mayor extracción que realizan los atacantes**




Fuente: Propia, adaptado de https://bit.ly/3zkxpKZ

Actualmente de acuerdo con la tendencia del 2020 (**Tabla 5**) dentro de las opciones de ciberataque se está utilizando técnicas *phishing* bancario más refinadas las cuales incluyen el uso de inteligencia artificial y la automatización del proceso a través de redes

[60] VEGA SÁNCHEZ, Op. cit., p.30

sociales. Lo anterior supone un nuevo reto para el personal de seguridad informática ya que muchas de estas técnicas y metodologías al ser automatizadas llegan a muchas personas en poco tiempo, se ejecutan y desaparecen muy rápido además borran cualquier rastro y/o su seguimiento es más complejo de analizar.

**Tabla 5. Tendencias de técnicas de ataques en Colombia durante el 2020**

| Técnicas | Descripción |
|---|---|
| Inteligencia artificial y *Malware* | Escaneo automatizado de vulnerabilidades con eliminado de evidencia digital |
| Uso de perfiles falsos en redes sociales para difusión de *malware* | Generación de contenido automatizado a través de cuentas falsas en redes sociales *Twitter* o *Facebook* con algún tipo de *malware* |
| BEC basado en *Deepfake* | Técnica que usa inteligencia artificial y que realiza el envío de contenido en audio o video suplantando a personal de la empresa, proveedores o clientes los cuales buscan que se haga transferencias de dinero por la adquisición de productos. |
| *Botnet* para difusión de correos electrónicos | Uso de correo masivo para envió de mensajería *phishing* o *spam* con tasa de envió de 30000 correos por hora. |
| Uso de mercados ilegales en *Darknet* | Venta de datos bancarios a través de internet profunda a través de foros de *Darknet* impulsados por el creciente uso de las criptomonedas las cuales no dejan trazabilidad a treves de un banco convencional |

Fuente: https://bit.ly/35Wc3qo

De allí en la actualidad según el reciente informe *Global Risk 2021*[61] los ciberataques y los fallos en los sistemas de las infraestructuras críticas se encuentran en el *Top* 5 de riesgos globales que publica cada año *el World Economic Forum* (*WEF*), es así como los ciberataques son temas de gran preocupación para este organismo ya que están entre los riesgos para tener en cuenta en la interconexión actual entre lo geopolítico, ambiental, social, económico y tecnológico.

[61] WORLD ECONOMIC FORUM. The Global Risks Report 2021 [sitio web]. Suiza; [Consultado: 07 de mayo de 2021]. Disponible en: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf

## 6.3 ESTABLECER LAS PRINCIPALES VULNERABILIDADES Y AMENAZAS QUE CONLLEVAN A LA EJECUCIÓN DE ATAQUES DE INGENIERÍA SOCIAL EN LAS EMPRESAS DEL SECTOR FINANCIERO Y ENTIDADES GUBERNAMENTALES COLOMBIANAS ENTRE LOS AÑOS 2015 Y 2020

A partir de la revisión bibliográfica a continuación se establecen las principales vulnerabilidades y amenazas que conllevan a la ejecución de ataques de ingeniería social en las empresas del sector financiero y entidades gubernamentales colombianas entre los años 2015 y 2020.

Para empezar, es de mencionar que es muy importante contar con el talento humano capacitado y actualizado para detectar fraudes, enfrentar una situación de ingeniería social puesto que estos son el frente por el cual llegan los ciberdelincuentes y además contar con profesionales de seguridad informática competentes con capacidad para atender de forma inmediata y dar tratamiento a las diferentes vulnerabilidades que se presenten en una entidad bancaria o gubernamental debido a que por su naturaleza manejan información muy sensible y evitar o actuar en el menor tiempo hace que no se comprometa los datos que confiaron clientes, proveedores y demás organizaciones. De igual manera la falta de sincronización, planeación y una adecuada gestión del sistema de seguridad informática propicia el ambiente idóneo para que muchas de las amenazas tengan un éxito y se propaguen rápidamente. Es por ello de gran importancia la evaluación y control de los riesgos a los cuales puede estar expuesta una entidad y así mitigar el impacto del mayor número posible de amenazas, además de conocer cuáles son las vulnerabilidades, abordarlas y tratar los riesgos antes que ocurran y puedan convertirse en una situación incontrolable, capaz de generar daños graves y poner en peligro la confidencialidad de la información. En la **Tabla 6** se pueden destacar algunas de las vulnerabilidades más comunes y por medio de las cuales los ciberdelincuentes pueden realizar ataques entre ellos ingeniería social.

**Tabla 6. Vulnerabilidades y amenazas para generar ataques de ingeniería social**

| Vulnerabilidades | Amenazas |
|---|---|
| Aceptar amigos sin conocer la procedencia o validación de su procedencia. | Fugas de información, acceso no autorizado a información confidencial de la empresa. |
| Uso de conexión a internet pública o insegura. | Interceptación de información (escucha) |
| Entrega de información de cuentas bancarias por parte de usuarios a través de correos electrónicos falsos o suplantados que adjuntan enlaces no oficiales. | Ingeniería social (picaresca) |
| Información compartida sin control de privacidad redes sociales por parte de los usuarios y empleados. | Fugas de información, acceso no autorizado a información confidencial de la empresa. |
| Contraseñas inseguras o poco robustas | Suplantación de identidad de usuario. |
| Problemas de seguridad informática en redes e infraestructura obsoleta, sin monitorear o sin configuración de acuerdo con políticas del sistema de gestión se seguridad informática (SGSI). | Interceptación de información (escucha), Denegación de servicios, acceso no autorizado. |
| Falta de capacitación a los empleados y usuarios en tecnologías de la información y las comunicaciones en temas de ataques de ingeniería social y uso de buenas prácticas de TI | Ingeniería social (picaresca) |

Fuente: Propia

Adicional a esto y teniendo en cuenta los trabajos realizados por Zambrano[62] en el 2019 se puede notar que una de las vulnerabilidades utilizadas para atacar es el correo

[62]ZAMBRANO, Angie y SUAREZ, Johan. La seguridad de las aplicaciones bancarias y dispositivos sin contacto que permiten efectuar pagos en Colombia [en línea]. Trabajo de grado. Bogotá. Universidad Militar Nueva Granada. Facultad de Relaciones Internacionales. Departamento de Administración de la seguridad

electrónico, medio por el cual los atacantes comparten *malware* haciendo uso del engaño e ingeniería social. Es una situación muy recurrente y por tal razón Zambrano[63] menciona una cifra entregada por *Kaspersky* donde alrededor de 430.000 usuarios fueron atacados y afectados con robos de dinero, criptomonedas y servicios de pago por internet, cifra que va en crecimiento y está un 7% más que el año inmediatamente anterior, sumado a esto hay un dato muy importante y es que el 30.9% de los ataques son a usuarios comerciales. Ahora bien, del total de casos de ciberataques 339.000 fueron ataques *phishing* que utilizaron la suplantación grandes entidades bancarias para engañar a las víctimas. Lo anterior muchos especialistas en seguridad lo conocen como *malware* financiero o troyanos bancarios ya que se especializan en robar a dinero y datos bancarios, esta técnica es de gran perjuicio para los bancos ya que con que un usuario que "muerda el anzuelo" del correo malicioso con *malware* y esté conectado en la red de un entorno corporativo, los demás equipos también serán susceptibles a infectarse en cuestión de minutos comprometiendo así mucha información en poco tiempo, en la **Tabla 7** se relacionan los programas maliciosos (*malware*) más populares en correos electrónicos *spam* y las páginas web de *phishing* utilizados para robar dinero y datos financieros de entornos corporativos.

y salud ocupacional, 2020. 80 p. [Consultado: 20 de mayo de 2021]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/36702/ZambranoLoaizaAngieCarolina-SuarezCastroJohanCamilo2020.pdf?sequence=1&isAllowed=y

[63] Ibid., p.47

**Tabla 7. Principales amenazas de *malware* en correos electrónicos *spam* y las páginas web de *phishing*.**

| ***Malware*** | **Familia** | **Objetivo** | **Usuario** | **Nivel de incidencia Amenaza (%)** | **Año** | **Descripción** |
|---|---|---|---|---|---|---|
| Troyano | Troyanos bancarios RTM | Sector bancario | Corporativo | 40 | 2018 | Cuando la víctima intenta realizar una transacción *online* el *malware* hace el reemplazo de datos de la cuenta y robar fondos manualmente. |
| Troyano | Troyanos bancarios *Emotet* | Sector bancario | Corporativo | 15 | 2019 | Envío de correo *phishing* con mensajes intrigantes o confusos y una vez ingresa al perímetro de la red este puede auto distribuirse por utilizando vulnerabilidades de equipos no parcheados para descargar nuevas amenazas. |
| Troyano | Troyanos bancarios *Trickster* | Sector bancario | Corporativo | 12 | 2019 | Envío de *malware* a través de correo electrónico para robo de credenciales bancarias y a su vez usa las cuentas del equipo infectado para hacer la propagación de nuevos correos, todo esto borrando evidencias en bandejas de entrada y salida. |

Fuente: https://bit.ly/35WiGt4

A su vez dentro de los principales datos buscados por los ciberdelincuentes dentro de un proceso de ataque están accesos a cuentas (usuario, contraseña), números de tarjetas de crédito y débito, tokens de seguridad y tarjetas de coordenadas de acuerdo con la **Tabla 8**, esto también tiene especial interés en las empresas objetivo de este estudio ya

que las entidades gubernamentales y bancos trabajan día a día con datos muy sensibles y con los cuales generan grandes centro de datos (Big Data), además el dinero que poseen es muy alto lo cual hace atractivo a este nicho del mercado pues los atacantes saben que si enfocan sus esfuerzos y conocimientos vean es posible tener un mayor "retorno de inversión" por así denominarlo y que no será una pérdida de tiempo y recursos.

**Tabla 8.** Información objetivo de ciberataques

| **Datos atacados** | **Nivel de recurrencia (%)** |
|---|---|
| Usuarios y contraseñas | 81 |
| Tarjetas de crédito | 46 |
| Tarjetas débito | 19 |
| Tokens | 9 |
| Tarjeta de coordenadas | 6 |

Fuente: Propia

Finalmente se puede concluir que un ataque logra materializarse por medio de la sincronización de diferentes herramientas y técnicas, muchas de las cuales hacen uso de redes sociales para obtener o recopilar información y establecer relaciones de confianza iniciales o perfilamientos y el correo electrónico para propagar *malware* o hace uso de *phishing* u otra técnica para hacer masivo el envío de *software* malicioso y materializar el ataque o redirección a entornos fraudulentos suplantando grandes empresas para obtener claves y datos bancarios o de información personal que les permita extraer recursos o chantajear a la victimas por dinero, acoso, dañar la reputación o intimidad entre otros.

## 6.4 CONSTRUIR UN DOCUMENTO CON RECOMENDACIONES QUE CONSOLIDE LAS PRINCIPALES TÉCNICAS, METODOLOGÍAS, VULNERABILIDADES Y AMENAZAS DE INGENIERÍA SOCIAL EN CORREOS ELECTRÓNICOS Y REDES SOCIALES DE EMPRESAS DEL SECTOR FINANCIERO Y ENTIDADES GUBERNAMENTALES COLOMBIANAS.

A continuación, en la **Tabla 9** se generan algunas recomendaciones de las principales técnicas, metodologías, vulnerabilidades y amenazas de Ingeniería social en correos electrónicos y redes sociales de empresas del sector financiero y entidades gubernamentales colombianas.

**Tabla 9.** Recomendaciones principales ataques de ingeniería social.

| Metodología | Técnica | Vulnerabilidades | Amenazas | Recomendaciones |
|---|---|---|---|---|
| Ingeniería social | *Phishing* | Falta de conocimiento y capacitación en tecnología e informática | Ingeniería social (picaresca) | Incluir y/o fortalecer dentro de las políticas del sistema de gestión y seguridad (SGSI) la capacitación a los empleados y personal usuario de las plataformas sobre el uso de las herramientas informáticas, sus riesgos y responsabilidades. Asimismo, formular políticas en apoyo de la dirección para la seguridad de la información y establecerla a toda la empresa empleados y a las partes externas pertinentes. |
| Ingeniería social | Inteligencia artificial y *Malware* | Escaneo automatizado de vulnerabilidades con eliminado de evidencia digital | Fugas de información, acceso no autorizado a información confidencial de la empresa. | Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. |
| Ingeniería social | Uso de perfiles falsos en redes sociales para difusión de *malware* | Generación de contenido automatizado a través de cuentas falsas en redes sociales *Twitter* o *Facebook* con algún tipo de *malware* | Acceso no autorizado, fugas de información | Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. |

Fuente: Propia

**Tabla 9.** (Continuación)

| Metodología | Técnica | Vulnerabilidades | Amenazas | Recomendaciones |
|---|---|---|---|---|
| Ingeniería social | BEC basado en *Deepfake* | Técnica que usa inteligencia artificial y que realiza el envío de contenido en audio o video suplantando a personal de la empresa, proveedores o clientes los cuales buscan que se haga transferencias de dinero por la adquisición de productos. | Ingeniería social (picaresca) | Incluir y/o fortalecer dentro de las políticas del sistema de gestión y seguridad (SGSI) la capacitación a los empleados y personal usuario de las plataformas sobre el uso de las herramientas informáticas, sus riesgos y responsabilidades. Asimismo, formular políticas en apoyo de la dirección para la seguridad de la información y establecerla a toda la empresa empleados y a las partes externas pertinentes. |
| Ingeniería social | *Botnet* para difusión de correos electrónicos | Uso de correo masivo para envió de mensajería *phishing* o *spam* con tasa de envió de 30000 correos por hora. | Acceso no autorizado, fugas de información | Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. |
| Ingeniería social | Uso de mercados ilegales en *Darknet* | Venta de datos bancarios a través de internet profunda a través de foros de *Darknet* impulsados por el creciente uso de las criptomonedas las cuales no dejan trazabilidad a treves de un banco convencional | Acceso no autorizado, fugas de información | Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos. |

Fuente: Propia

Frente a los diferentes tipos de amenazas es posible mitigarlas teniendo en cuenta las siguientes etapas.

- **Prevención**. Además de las medidas de protección física y lógica es importante que el talento humano y los usuarios de las plataformas tengan siempre de primera mano la información de las últimas técnicas de ciberataques y que cuenten con la capacitación de uso adecuado de las diferentes herramientas informáticas.

- **Detección.** Para garantizar la seguridad es necesario gestionar las vulnerabilidades y realizar monitoreo continuo. A su vez es una buena política tener configurado de forma correcta los sistemas antivirus y sistemas de seguridad perimetral para detectar posibles amenazas y evitar que los hackers puedan actuar sin ser detectados por varios días y generar mayor daño. Cuando los ataques no pueden ser detectados de forma inmediata por los sistemas de seguridad las afectaciones son mayores ya que de acuerdo con Monsalve[64] se ha podido documentar que desde que el atacante rompe la brecha de seguridad y la detección pasan alrededor de 205 días.

- **Reacción y respuesta.** Si se generó un ataque el primer paso es generar una respuesta técnica y si hay datos comprometidos el siguiente paso es reportar ante las instituciones oficiales como el CAI Virtual de la policía nacional para radicar la respectiva denuncia. En cuanto a la respuesta técnica es necesario actuar para mitigar el impacto y para lo cual se debe desconectar al equipo de conexiones a internet, si no hay antivirus instalar uno y realizar un escaneo completo del sistema y finalmente realizar cambios de contraseñas y analizar datos manualmente quitando aquellos que no hacían parte del sistema.

[64] MONSALVE MENDEZ, Op.cit., p.2.

Es muy importante que desde la seguridad informática se incluya y se de gran atención al talento humano y usuarios de las diferentes plataformas en aras de controlar vulnerabilidades, amenazas y riesgos de gran impacto en un sistema informático ya que si se aplica ingeniería social un atacante podrá traspasar el esquema de seguridad de cualquier infraestructura por robusta que esta sea.

# 7. CONCLUSIONES

Entre el 2015 y 2020 los ataques de ingeniería social continúan en crecimiento, es así como durante el 2020, época de pandemia los casos de ataques de ingeniería social en correos electrónicos y redes sociales representaron una de las grandes amenazas para la seguridad de la información de las empresas, principalmente para el sector financiero y entidades gubernamentales colombianas, muchos de los cuales están sustentados en el engaño de las personas.

Dentro de las técnicas y metodologías de Ingeniería social en correos electrónicos y redes sociales de empresas del sector financiero y entidades gubernamentales colombianas se puede observar que la técnica más utilizada es el *phishing* a través de Ingeniería social, la cual utiliza las redes sociales para realizar perfilamiento, reconocimiento y análisis de las víctima, mientras que la ejecución del plan final está apoyado en correos electrónicos con suplantación de identidad corporativa y camuflándose para lograr que la víctima no tenga sospecha y acceda a sus peticiones. Actualmente se han fortalecido los ataques a través de redes sociales, aprovechando que muchos usuarios las usan para distraerse y comunicarse con otras personas, además de que muchos no usan claves seguras y/o configuraciones a para restringir el acceso o desconocen la forma de realizarlo.

Una de las principales vulnerabilidades que conlleva a la ejecución de ataques de ingeniería social en las empresas del sector financiero y entidades gubernamentales colombianas es la falta de capacitación de las personas y la adopción de conductas responsables frente al uso de las diferentes plataformas instituciones. Existe una gran amenaza donde se ve comprometida información sensible entre los que se encuentran datos personales, información financiera y datos bancarios.

Frente a todos estos tipos de ataques de ingeniería social el uso de internet con cautela, dudar frente a cualquier acción y preguntarse “esto es verdad, es confiable y real” o si

por el contrario no es prudente ingresar datos o dar clics es primordial para asegurar la información sensible o privada. De otro modo las redes sociales debe ser un medio de uso consciente y responsable, medir cual es el grado de vulnerabilidad y consignar información solamente necesaria, si se tratan de datos sensibles o de empresas se debe realizar la correcta configuración de la privacidad y evitar aceptar invitaciones de personas desconocidas.

# 8. RECOMENDACIONES

Una recomendación que es importante tener en cuenta para generar trazabilidad a lo largo del tiempo, es continuar realizando estudios en ingeniería social en empresas y así poder conocer en el comportamiento de los nuevos ataques de ingeniera social y las estrategias que adopten los ciberdelincuentes y las empresas para contrarrestarlos o mitigarlos.

Continuar con estudios de análisis de ataques generados por redes sociales y correos electrónicos en las empresas, ya que permiten conocer vulnerabilidades y amenazas valiosas para el análisis de tendencias de ciberataques y hacer gestión del riesgo informático de estas. Además, a nivel cuantitativo se puede realizar una medición del número de posibles relaciones existentes entre los involucrados, como también la dirección y profundidad de la ciberdelincuencia.

Fortalecer los espacios de formación, desarrollo e intercambio de conocimiento a nivel intra e interinstitucional, en áreas como seguridad informática, técnicas de ataques de ingeniería social, los mismos que sirvan para generar conciencia y prevención en nuevos ataques que faciliten la transferencia de conocimiento a nivel académico, social y empresarial.

Potenciar la relación entre el talento humano y la empresa en pro de conocer las fortalezas, debilidades y el impacto que estos puedan generar sobre la seguridad de la información y su confidencialidad. Es importante centrar estrategias para la enseñanza activa y constructiva en temas de ciberseguridad que permitan fortalecer el sentido de pertenencia de la información y el uso responsable de toda la infraestructura de TI, para así mitigar vulnerabilidades, dar tratamiento a las amenazas y hacer una correcta gestión del riesgo.

## BIBLIOGRAFÍA

ACOSTA PINEDA, Santiago et al. Ingeniería social en instituciones de educación superior. En: Tecnologías de avanzada [en línea]. Norte de Santander: Revista Colombiana de Tecnologías de Avanzada, abril-junio de 2018, vol., 2, nro. 32. 10 p. [Consultado: 23 de septiembre de 2020]. Disponible en http://revistas.unipamplona.edu.co/ojs_viceinves/index.php/RCTA/article/view/2370/0. ISSN 1692-7257

ARENAS BONILLA, Oscar Javier. El eslabón más débil [en línea]. Trabajo de grado especialización en Seguridad Informática. Bogotá. Universidad Piloto de Colombia. Facultad de Ingeniería. Departamento de ingeniería de sistemas, 2016. 8 p. [Consultado: 17 de julio de 2021]. Disponible en: http://polux.unipiloto.edu.co:8080/00001933.pdf

BENAVIDES ASTUDILLO, Eduardo. Un experimento para crear conciencia en las personas acerca de los ataques de Ingeniería Social. En: Ciencia: Revista UNEMI [en línea]. Milagro: Universidad Estatal de Milagro, enero-abril de 2020. vol. 13, nro. 32. p. 27 - 40. [Consultado: 13 de noviembre de 2020]. Disponible en http://ojs.unemi.edu.ec/index.php/cienciaunemi/article/view/1028/1003. E-ISSN: 2528-7737.

BERMUDEZ PENAGOS, Edilberto. Ingeniería social, un factor de riesgo informático inminente en la Universidad Cooperativa De Colombia sede Neiva [en línea]. Trabajo de grado especialización en seguridad informática. Neiva. Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Ingeniería de sistemas. Departamento de sistemas, 2015. 116 p. [Consultado: 16 de noviembre de 2020]. Disponible en: Repositorio Educativo Digital UAO. https://repository.unad.edu.co/handle/10596/3629

CARRILLO LUQUE, Vicente y SÁNCHEZ PASTOR, Fernando. La ingeniería social aplicada al delito informático. una aproximación [en línea]. Universidad Complutense de Madrid. Facultad de informática. Departamento de Sistemas Informáticos y Computación, 2011. 57 p. [Consultado: 24 de septiembre de 2020]. Disponible en: http://www.simulador*online*.es/descargas/La_Ingenieria_social_Aplicada_al_Delito_Informatico_Una_Aproximacion.pdf

CARVAJAL, Hernán Darío y CASTELLANOS, John. Ataque controlado de ingeniería social usando códigos QR [en línea]. Trabajo de grado especialización en seguridad de la información. Bogotá. Universidad Católica de Colombia. Facultad de ingeniería. Departamento de Sistemas, 2019. 98 p. [Consultado: 12 de noviembre de 2020]. Disponible en: Repositorio Educativo Digital UCATOLICA. https://repository.ucatolica.edu.co/jspui/handle/10983/24063

CONGRESO DE LA REPÚBLICA DE COLOMBIA, SENADO. Ley 1273 de 2009 [sitio web]. Bogotá; [Consultado: 28 de septiembre de 2020]. Disponible en: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

CORTES HERNANDEZ, Andrés. Ingeniería social: *Phishing* y *Baiting* [en línea]. Trabajo de grado Especialización en Seguridad Informática. Bogotá. Universidad Piloto de Colombia. Facultad de ingenierías. Departamento de sistemas, 2019. 10 p. [Consultado: 2 de octubre de 2020]. Disponible en: Repositorio Educativo Digital UNIPILOTO. http://repository.unipiloto.edu.co/handle/20.500.12277/6349

DE SALVADOR, Luis. Ingeniería Social y Operaciones psicológicas en internet [en línea]. Ieee.es. (18 de octubre de 2011). [Consultado: 2 de octubre de 2020]. Disponible en Internet: http://www.ieee.es/Galerias/fichero/docs_opinion/2011/DIEEEO74-2011.IngenieriaSocial_LuisdeSalvador.pdf

ESET; Security report; Latinoamérica 2015; [sitio web]. Latinoamérica: ESET. [Consultado: 20 de mayo de 2021]. Disponible en: https://www.welivesecurity.com/wp-content/uploads/2015/03/ESET_security_report_2015.pdf

ESTRADA ESPONDA, Royer David. Prácticas de seguridad de información del Nivel Ejecutivo de la Policía Nacional de Colombia en la Escuela de Policía Simón Bolívar (Tuluá, Colombia). En: Ciencia y Tecnología estudio de caso [en línea]. Logos: Policía Nacional de Colombia, enero-abril de 2020, vol. 12, nro. 1. 131 p. [Consultado: 13 de noviembre de 2020]. Disponible en https://revistalogos.policia.edu.co:8443/index.php/rlct/article/view/1050. ISSN 0121-0777.

FIGUEROA SUÁREZ, Juan. La seguridad informática y la seguridad de la información. En: Casa editora del Polo: Revista Polo del conocimiento [en línea]. Ecuador: Casa editora del Polo, noviembre-diciembre de 2017. Ed. 14, vol. 2, nro.12. p. 3-4. [Consultado: 08 de mayo de 2021]. Disponible en https://polodelconocimiento.com/ojs/index.php/es/article/view/420/pdf. ISSN: 2550-682X.

FLOREZ RAMIREZ, Claudia Patricia y MÉNDEZ COLLO Harold. Estudio de ingeniería social en el uso de las redes sociales [en línea]. Trabajo de grado especialización en seguridad informática. Bogotá. Universidad Nacional Abierta y a Distancia UNAD. Escuela de ciencias básicas, tecnología e ingeniería. Departamento de Ingeniería de Sistemas, 2017. 129 p. [Consultado: 16 de noviembre de 2020]. Disponible en: Repositorio Educativo Digital UNAD. https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/14505/1/17659358.pdf

GARCÍA, Constanza. Economía digital [en línea]. BBVA. Colombia. (19 de septiembre de 2019). [Consultado: 2 de octubre de 2020]. Disponible en:

https://www.bbva.com/es/co/colombia-llegara-a-los-32-millones-de-usuarios-de-internet-en-2020/

GIRALDO MARTINEZ, Jenny Paola y PACHECO DUARTE, Iván Guillermo. Ingeniera social: técnica de ataque *phishing* y su impacto en las empresas colombianas [en línea]. Trabajo de grado especialización en seguridad informática. Salamina. Universidad Nacional Abierta y a Distancia - UNAD. Facultad de ingeniería y ciencias básicas. Departamento de sistemas, 2018. 90 p. [Consultado: 10 de noviembre de 2020]. Disponible en: Repositorio Educativo Digital UNAD. https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/27050/1/jpgiraldoma.pdf

GOMÉZ VIEITES, Álvaro. Enciclopedia de la Seguridad Informática. Segunda edición. Madrid, España: Editorial RA-MA. 2017. 1085 p. ISBN: 9788499640385

GOBIERNO DE ESPAÑA, INCIBE. *Phishing* [sitio web]. Madrid; [Consultado: 07 de mayo de 2021]. Disponible en: https://www.incibe.es/aprendeciberseguridad/*phishing*

GOBIERNO DE ESPAÑA, INCIBE. Detección de APTs [sitio web]. España; [Consultado: 07 de mayo de 2021]. Disponible en: https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/deteccion_apt.pdf

HÜTT HERRERA, Harold. Las redes sociales: Una nueva herramienta de difusión. En: Redalyc: Revista Reflexiones [en línea]. Costa Rica: Universidad de Costa Rica, enero-junio de 2011. vol. 91, nro. 2. p. 121-128. [Consultado: 23 de septiembre de 2020]. Disponible en https://www.redalyc.org/pdf/729/72923962008.pdf. E-ISSN: 1021-1209.

*KASPERSKY*, CENTRO DE RECURSOS. Virus informáticos y *Malware* [sitio web]. América latina; [Consultado: 07 de mayo de 2021]. Disponible en:

https://latam.*Kaspersky*.com/resource-center/threats/computer-viruses-and-*malware*-facts-and-faqs

LEGUIZAMON, Maira Sheila. El *Phishing* [en línea]. Trabajo final de grado en criminología y seguridad. Castellón de la Plana. Universidad Jaime I. Escuela Superior de Tecnología y Ciencias Experimentales. Departamento de Lenguajes y Sistemas Informáticos, 2015. 47p. [Consultado: 10 de septiembre de 2020]. Disponible en: Repositorio Educativo Digital UJI. http://hdl.handle.net/10234/127507

LÓPEZ ALONSO, Covadonga. El correo electrónico. En: Estudios de lingüística del español [en línea]. Covadonga López Alonso: Universidad Complutense de Madrid, enero-junio de 2006. vol. 24. p. 1-3. [Consultado: 30 de septiembre de 2020]. Disponible en https://www.raco.cat/index.php/Elies/article/view/195637

LÓPEZ GRANDE, Carlos et al. Ingeniería social: El ataque silencioso. En: ITCA-FEPAD [en línea]. El salvador: Revista Tecnológica de Escuela Especializada en Ingeniería, enero-diciembre de 2015, vol., 2, nro. 8. 8 p. [Consultado: 7 de octubre de 2020]. Disponible http://hdl.handle.net/10972/2910.

LÓPEZ VILLA, Oscar David. Análisis y desarrollo de estrategias para la prevención del uso de la ingeniería social en la sociedad de la información. En: Ingenierías: Revista Ingenierías USBMed [en línea]. Medellín: Universidad de San Buenaventura, julio-diciembre de 2013. vol. 4, nro. 2. p. 1-7. [Consultado: 2 de octubre de 2020]. Disponible en http://revistas.usbbog.edu.co/index.php/IngUSBmed/article/view/287/202. E-ISSN: 2027-5846.

MARIN JIMENEZ, Rafael. Estudio de metodologías de ingeniería social [en línea]. Trabajo de grado Master Interuniversitario en seguridad de las tecnologías de la información y las comunicaciones. Barcelona. Universitat Oberta de Catalunya (UOC). Facultad de Informática, Multimedia y Telecomunicación. Departamento de informática,

2018. 133 p. [Consultado: 26 de septiembre de 2020]. Disponible en: Repositorio Educativo Digital UOC. http://hdl.handle.net/10609/81271

MIGUEL PEREZ, Julio Cesar. Protección de datos y seguridad de la información [en línea]. 4 ed. Madrid: RA-MA. 2015, 271 p. [Consultado el 26 de septiembre de 2020]. Disponible en: Base de datos libros Google. https://books.google.com.co/books?id=To6fDwAAQBAJ&lpg=PA1&hl=es&pg=PA1#v=onepage&q&f=false ISBN 978-84-9964-560-5.

MONSALVE MENDEZ, Jaime Yesid. Ciberseguridad: Principales amenazas en Colombia (Ingeniera social, *Phishing* y DDoS) [en línea]. Trabajo de grado especialización en seguridad informática. Bogotá. Universidad Piloto de Colombia. 2018. 75 p. [Consultado: 20 de mayo de 2021]. Disponible en: Repositorio Educativo Digital. http://repository.unipiloto.edu.co/handle/20.500.12277/4663

OLIVARES SERRANO, Javier. Seguridad informática: *Hacking* Ético. [en línea]. 4 ed. Barcelona: Ediciones ENI. 2018, 810 p. [Consultado el 25 de septiembre de 2020]. Disponible en: https://catoute.unileon.es/permalink/34BUC_ULE/1ekdeev/alma991000306699705772. Epsilon.ISBN: 978-2-409-01297-6.

OSI. Aprendiendo a identificar fraudes *online* [sitio web]. España; [Consultado: 06 de agosto de 2021]. Disponible en: https://www.osi.es/es/guia-fraudes-*online*

PARDO FERRO, Carlos Enrique. Amenazas en la red: entrando al mundo de los ciberataques - ingeniería social, *phishing* y *malware* [en línea]. Trabajo de grado especialización en Seguridad Informática. Bogotá. Universidad Piloto de Colombia. Facultad de Ingeniería. Departamento de ingeniería de sistemas, 2018. 12 p. [Consultado: 9 de noviembre de 2020]. Disponible en: Repositorio Educativo Digital UNIPILOTO. http://repository.unipiloto.edu.co/handle/20.500.12277/2647

PLAZAS GARCIA, Edna Rocio. Ingeniera social: en las empresas colombianas [en línea]. Trabajo de grado especialización en seguridad informática. Pitalito. Universidad Nacional Abierta y a Distancia - UNAD. Facultad de ingeniería y ciencias básicas. Departamento de sistemas, 2018. 75 p. [Consultado: 20 de mayo de 2021]. Disponible en: Repositorio Educativo Digital UNAD. https://repository.unad.edu.co/handle/10596/18704

PEREZ, Yolman. Un caso de *phishing* más en Colombia [en línea]. Sala de conocimiento Universidad Cooperativa de Colombia. Arauca. (25 de abril de 2017). [Consultado: 15 de noviembre de 2020]. Disponible en: https://www.ucc.edu.co/prensa/2016/Paginas/un-caso-de-*phishing*-mas-en-colombia.aspx

POLICIA NACIONAL DE COLOMBIA [sitio web]. Bogotá. CAI VIRTUAL. Balance Cibercrimen 2020. [Consultado: 18 de mayo de 2021]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/balance_cibercrimen_2020_-_semana_45.pdf

POLICIA NACIONAL DE COLOMBIA [sitio web]. Bogotá. CAI VIRTUAL. Tendencias Cibercrimen en Colombia. [Consultado: 20 de septiembre de 2020]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/tendencias_cibercrimen_colombia_2019_-_2020_0.pdf

ROMERO RUBIO, Diego Alexander. El arte de la ingeniería social [en línea]. Trabajo de grado Especialización de seguridad informática. Bogotá. Universidad piloto de Colombia. Facultad de ingeniería. Departamento de sistemas, 2019. 10 p. [Consultado: 2 de octubre de 2020]. Disponible en: Repositorio Educativo Digital UNIPILOTO. http://repository.unipiloto.edu.co/handle/20.500.12277/6354

SANCHEZ, PATARROYO, Henry. Ingeniería social, una técnica subestimada por desconocimiento [en línea]. Trabajo de grado Especialización en Seguridad Informática.

Bogotá. Universidad Piloto de Colombia. Facultad de ingenierías. Departamento de sistemas, 2016. 8 p. [Consultado: 25 de septiembre de 2020]. Disponible en: Repositorio Educativo Digital UNIPILOTO. http://repository.unipiloto.edu.co/handle/20.500.12277/4934

SERGIO ARCOS, Sebastián. Ingeniería social: Psicología aplicada a la seguridad informática [en línea]. Trabajo de grado Ingeniería en Informática. Barcelona. Universidad Politécnica de Cataluña. Facultad de Ingeniería. Departamento de Ingeniería de Servicios y Sistemas de Información, 2011. 142 p. [Consultado: 25 de septiembre de 2020]. Disponible en: Repositorio Educativo Digital UPC. http://hdl.handle.net/2099.1/12289

SUPERINTENDECIA DE INDUSTRIA Y COMERCIO. Protección de Datos Personales [sitio web]. Bogotá; [Consultado: 28 de septiembre de 2020]. Disponible en: https://www.sic.gov.co/sobre-la-proteccion-de-datos-personales

TORRES DIAZ, Oswaldo Alejandro. Diseño e implementación de un plan de concientización frente a la ingeniería social para la empresa promociones y cobranzas beta s.a. [en línea]. Trabajo de grado para optar al título de Especialista en Seguridad Informática. Bogotá. Universidad Piloto de Colombia. Facultad de posgrados de ingeniería. Departamento de sistemas, 2017. 188 p. [Consultado: 2 de octubre de 2020]. Disponible en: Repositorio Educativo Digital UNIPILOTO. http://repository.unipiloto.edu.co/handle/20.500.12277/2769

VEGA SÁNCHEZ, Fabio Alexander y SUARÉZ LIZCANO, Wilson. Métodos de ataques y prevención de la ingeniería social en las alcaldías del huila en Colombia [en línea]. Trabajo de grado especialización en seguridad informática. Neiva. Universidad Nacional Abierta y a Distancia - UNAD. Facultad de ingeniería y ciencias básicas. Departamento de sistemas, 2018. 85 p. [Consultado: 24 de mayo de 2021]. Disponible en: Repositorio Educativo Digital UNAD. https://repository.unad.edu.co/handle/10596/18701

ZABALA, Jhon Alexander. Responsabilidad bancaria frente al delito de *phishing* en Colombia [en línea]. Trabajo de grado Pregrado en Derecho. Bogotá. Universidad Católica de Colombia. Facultad de Ciencias Sociales y políticas. Departamento de derecho, 2017. 26 p. [Consultado: 16 de noviembre de 2020]. Disponible en: Repositorio Educativo Digital UCATOLICA. http://hdl.handle.net/10983/14943

ZAMBRANO, Angie y SUAREZ, Johan. La seguridad de las aplicaciones bancarias y dispositivos sin contacto que permiten efectuar pagos en Colombia [en línea]. Trabajo de grado. Bogotá. Universidad Militar Nueva Granada. Facultad de Relaciones Internacionales. Departamento de Administración de la seguridad y salud ocupacional, 2020. 80 p. [Consultado: 20 de mayo de 2021]. Disponible en: https://repository.unimilitar.edu.co/bitstream/handle/10654/36702/ZambranoLoaizaAngieCarolina-SuarezCastroJohanCamilo2020.pdf?sequence=1&isAllowed=y

WORLD ECONOMIC FORUM. The Global Risks Report 2021 [sitio web]. Suiza; [Consultado: 07 de mayo de 2021]. Disponible en: http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf