IMPACTO DE LOS ATAQUES DE INGENIERÍA SOCIAL EN COLOMBIA DESDE EL AÑO 2016 HASTA EL AÑO 2019.

PAOLA MARITZA RINCÓN NUÑEZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
DUITAMA
2021

IMPACTO DE LOS ATAQUES DE INGENIERÍA SOCIAL EN COLOMBIA DESDE EL AÑO 2016 HASTA EL AÑO 2019.

PAOLA MARITZA RINCÓN NUÑEZ

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

Director Proyecto
Esp. Ing. DANIEL FELIPE PALOMO LUNA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
DUITAMA
2021

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Duitama. 03 de junio de 2021

DEDICATORIA

Llena de satisfacción y esperanza con mucho amor dedico este trabajo a mis hijos, que con su cariño y apoyo me acompañan en esta etapa de mi vida, sin dejar a un lado a mis seres queridos; también lo dedico a mi mamá que con su apoyo, consagración y paciencia contribuyo a que pudiera alcanzar este logro, Mamita cada palabra de aliento, cada momento de bendiciones llenan mi vida. Con su sabiduría formó un cimiento lleno de confianza para seguir cada día adelante.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD, quienes con su trabajo continuo nos brindan la oportunidad de estudiar y laborar, por otro lado, a cada uno de los tutores y asesores que me acompañaron en el proceso les reconozco que sin su apoyo y colaboración éste logro no hubiera sido posible.

CONTENIDO

pág.

1. INTRODUCCIÓN 16
1. DEFINICIÓN DEL PROBLEMA 18
1.1 ANTECEDENTES DEL PROBLEMA 18
1.2 FORMULACIÓN DEL PROBLEMA 19
2. JUSTIFICACIÓN 20
3. OBJETIVOS 22
3.1 OBJETIVOS GENERAL 22
3.2 OBJETIVOS ESPECÍFICOS 22
4. MARCO REFERENCIAL 23
4.1 MARCO TEÓRICO 23
4.1.1 Phishing 26
4.1.2 Smishing 27
4.1.3 Vishing 28
4.1.4 Impersonation 29
4.2 MARCO CONCEPTUAL 29
4.2.1 Spear phishing 32
4.2.2 Baiting 33
4.2.3 Watering hole attack. 33
4.2.4 Quid pro quo 33
4.3 MARCO LEGAL 34
4.3.1 CONPES 3701 37
4.3.2 CONPES 3854 37
5. DESARROLLO DE LOS OBJETIVOS 38
5.1 Origen y evolucion de los ataques de ingeniería social 38
5.1.1 Phishing general. Phishing tradicional, Bulk Phishing o Spray and pray. 39

5.1.2 Vishing 39
5.1.3 Smishing..... 40
5.1.4 URL Phishing 40
5.1.5 Whaling 41
5.1.6 Business Email Compromise (BEC) o estafas Man-in-the-Email 41
5.1.7 CEO Fraud 42
5.1.8 Spear Phishing 42
5.1.9 Search Engine phishing..... 43
5.1.10 Phising con evasión de filtros. 44
5.1.11 Pharming o DNS-Based Phishing..... 44
5.1.12 Malware-based phishing..... 45
5.1.13 Content-Injection phishing 45
5.1.14 Watering Hole Phishing, watering hole attack. 45
5.1.15 Evil Twin 46
5.1.16 Social Network Phishing 46
5.1.17 Phishing 2.0..... 46
5.1.18 Hishing o “hardware phishing”. 47

5.2 Evolución de la ingeniería social 47

5.3 Ataques de ingeniería social más utilizados en Colombia 51

5.4 Estratégias propuestas por parte de las entidades del estado colombiano para la mitigación de los ataques de ingeniería social 59

5.5 BUENAS PRÁCTICAS Y RECOMENDACIONES PARA QUE LAS PERSONAS NO SE VEAN AFECTADAS POR ATAQUES DE INGENIERÍA SOCIAL..... 63
5.5.1 Estafa 63
5.5.2 Phishing 65
5.5.3 Suplantación..... 71
5.5.4 Vishing 72
5.5.5 Smishing..... 73
5.5.6 Carta nigeriana 74

6. CONCLUSIONES 75

7. RECOMENDACIONES 77

BIBLIOGRAFÍA 78

ANEXOS 84

LISTA DE FIGURAS

pág.

Figura 1. Principios de la seguridad de la información. 24
Figura 2. *Phishing* entidad bancaria. 26
Figura 3. *Smishing* ejemplo de estafa. 27
Figura 4. Ilustración *Vishing*. 28
Figura 5. *BEC*. 42
Figura 6. *Search engine phishing*. 44
Figura 7. Línea de tiempo ingeniería social. 48
Figura 8. *Phishing AOL Mail*. 50
Figura 9. Delitos reportados en 2016. 52
Figura 10. Delitos informáticos denunciados en 2016 52
Figura 11. Delitos reportados en 2017. 53
Figura 12. Delitos informáticos denunciados en 2017 53
Figura 13. Delitos reportados en 2018. 54
Figura 14. Delitos informáticos denunciados en 2018 54
Figura 15. Delitos reportados en 2019. 55
Figura 16. Delitos informáticos denunciados en 2019 55
Figura 17. Delitos informáticos denunciados en 2016-2019 56
Figura 18. Delitos informáticos relacionados a la IS 2016-2019 57
Figura 19. Principales vectores de ataque en 2019. 58
Figura 20. Ejemplo de *phishing* 65
Figura 21. Formulario creado por el atacante 67

LISTA DE CUADROS

pág.

Cuadro 1. Amenazas y vulnerabilidades 31

LISTA DE ANEXOS

pág.

Anexo A. Resumen Analítica Especializado -RAE. 85

GLOSARIO

ADWARE: *software* instalado normalmente de manera involuntaria, que permite el envío de publicidad a un usuario o equipo.

AMENAZA: causa u origen de un potencial incidente, mediante el cual es posible causar daño a un sistema de información o a una organización.

ANTISPAM: son productos, herramientas, servicios o funcionalidades que se encargan de evitar la recepción de correos no solicitados, ni deseados. Generalmente contienen información publicitaria o engañosa.

APLICACIONES ENGAÑOSAS: *software* que se promueve para realizar una función específica, pero realmente instala en segundo plano *malware* o código malicioso. Esto se hace con el objetivo de comprometer el sistema o recopilar información para enviar a un tercero.

BOTNET: "conjunto o red de robots (equipos o dispositivos) que son controlados por el atacante. Cuando un equipo de cómputo es infectado, pasa a formar parte de esta red con el fin de que el atacante lo utilice para los fines que él necesita; por lo general, las botnets son utilizadas para enviar spam"[1].

BUSINESS EMAIL COMPROMISE (BEC): ataque que hace uso de correos electrónicos corporativos comprometidos para ejecutar fraudes a organizaciones comerciales o gubernamentales.

CLICKBAIT: La URL de un sitio web o un archivo adjunto de correo electrónico que parece provenir de una fuente confiable, pero que en realidad está conectado a una fuente configurada por un pirata informático. "Las URL de clickbait o los archivos adjuntos suelen tener títulos atractivos como "aumento de salario" o "foto tuya en la fiesta", que incitan la curiosidad humana"[2].

*DARKNET: "*red utilizada para enrutar contenido, en la que todos los servicios y sitios son accesibles solo mediante direcciones no enrutables globalmente o solo a

[1] LÓPEZ GRANDE, Carlos Edgardo y SALVADOR GUADRÓN, Ricardo. Ingeniería Social: El Ataque Silencioso [en línea]. 2015, enero –diciembre, vol.7, nro.1. [Consultado 12 de enero 2021]. ISSN 2072-568X. Disponible en: http://www.redicces.org.sv/jspui/bitstream/10972/2910/1/Articulo6.pdf

[2] SECURECLICK. Glosario de términos de ingeniería social y seguridad de la información de AZ. [Sitio Web]. [Consulta: 22 de enero de 2021]. Disponible en: https://www.itsecurityawareness.ie/a-z-glossary-of-information-security-and-social-engineering-terms

través de redes superpuestas como *Tor, The Invisible Internet Project* (I2P) o *FreeNet*"[3].

*DEEPFAKE: "*usado genéricamente por los medios para referirse a cualquier video en el que las caras han sido intercambiadas o alteradas digitalmente, con la ayuda de Inteligencia Artificial"[4].

HTTP (Hypertext Transfer Protocol): es un protocolo donde se utiliza un sistema mediante el cual se permite la transferencia de información entre diferentes servicios y los clientes que utilizan páginas *web*.

INGENIERÍA SOCIAL: puede definirse esencialmente como el uso de las relaciones humanas para lograr un objetivo[5], también como un grupo de técnicas de tipo social que pueden ser usadas por ciertas personas o grupos; con el fin de manipular o persuadir a objetivos humanos, esto para que realicen acciones, tomen decisiones o en determinado caso revelen información sensible al atacante voluntariamente.

MALWARE: abreviatura de *software* malicioso, generalmente consiste en código desarrollado por ciberatacantes, diseñado para causar daños extensos a los datos y sistemas o para obtener acceso no autorizado a una red. "el *malware* generalmente se entrega en forma de enlace o archivo por correo electrónico y requiere que el usuario haga clic en el enlace o abra el archivo para ejecutarlo"[6].

PHARMING: es una "técnica para desviar a los usuarios a sitios fraudulentos o servidores proxy, generalmente a través del secuestro o envenenamiento de DNS"[7], lo cual requiere que se realice una manipulación técnica sobre las direcciones DNS utilizadas por un usuario, esto con el fin de redirigir la navegación a sitios web que muestran un aspecto idéntico, pero que no son los auténticos y han sido creados con fines fraudulentos.

PHISHING: método de ingeniería social basado en el engaño y diseñado para suplantar un servicio legítimo, con el fin de que el usuario proporcione información confidencial.

---

[3] ARGONNE. DarkNet Terminology: Definitions of the DarkNet, the Dark Web, and the Deep Web. [Sitio Web]. [Consulta: 22 de enero de 2021]. Disponible en: https://coar.risc.anl.gov/coar-attends-department-of-homeland-security-hosted-darknet-summit/

[4] BBC. Deepfakes: What are they and why would I make one? [Sitio Web]. [Consulta: 22 de enero de 2021]. Disponible en: https://www.bbc.co.uk/bitesize/articles/zfkwcqt

[5] DOLAN, Aaron, Social Engineering. [Sitio Web]. [Consulta: 1 de junio de 2021]. Disponible en: https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-1365

[6] FORCEPOINT. What is Malware? Malware Defined, Explained, and Explored. [Sitio Web]. [Consulta: 22 de enero de 2021]. Disponible en: https://www.forcepoint.com/es/cyber-edu/malware

[7] NOHLBERG, Marcus, Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks. Estocolmo. Universitetsservice US-AB. 2018. p.59. ISBN 978-91-7155-786-5

RANSOMWARE: “software malicioso que infecta y le da al atacante la posibilidad de bloquear un equipo informático y controlar sus datos”[8].

SMISHING: se refiere a ataques de phishing que implican el uso de mensajes enviados mediante SMS (Servicio de mensajes cortos). “Los mensajes de texto falsos son recibidos por posibles víctimas, quienes a su vez responden directamente o visitan un sitio web de phishing”[9].

SPEAR PHISING: es una estafa por correo o comunicaciones electrónicos que es dirigida a una persona, organización o empresa específica. “A menudo tienen la intención de robar datos con fines maliciosos, los ciberdelincuentes también pueden intentar instalar software malicioso en el computador o dispositivo del usuario objetivo”[10].

SPYWARE: “tipo de *software* malicioso que intenta mantenerse oculto mientras registra información en secreto y sigue sus actividades en línea, tanto en equipos como en dispositivos móviles. Puede tener la capacidad de supervisar y copiar todo lo que escribe, carga, descarga y almacena”[11].

URL (Uniform Resource Locator): es la dirección específica que se asigna a cada uno de los recursos disponibles en la red con la finalidad de que estos puedan ser localizados o identificados.

VISHING: es solo una forma de phishing, que es cualquier tipo de mensaje, como un correo electrónico, texto, llamada telefónica o mensaje de chat directo, que parece provenir de una fuente confiable o legitima, pero no lo es, “cuyo objetivo es robar la identidad o el dinero de alguien, en este caso mediante una llamada telefónica”[12].

WHALING: también conocido como: *whaling phishing* o *whaling phishing attack*, “es un tipo específico de ataque de *phishing* que tiene como objetivo a empleados de alto perfil, como el director ejecutivo o el director financiero, para robar información confidencial de una empresa”[13].

---

[8] PONS GAMÓN. A. Vicente. Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. [en línea]. [Consulta: 22 de enero de 2021]. Disponible en: https://www.redalyc.org/jatsRepo/5526/552656641007/index.html

[9] TREND MICRO. Smishing. [Sitio Web]. [Consulta: 22 de enero de 2021]. Disponible en: https://www.trendmicro.com/vinfo/us/security/definition/smishing

[10] KASPERSKY. What is Spear Phishing? [en línea]. [Consulta: 23 de enero de 2021]. Disponible en: https://www.kaspersky.com/resource-center/definitions/spear-phishing

[11] AVAST. ¿Qué es el spyware? [Sitio Web]. Patrick Seguin. [Consulta: 20 de enero de 2021]. Disponible en: https://www.avast.com/es-es/c-spyware

[12] NORTON. What is vishing? Tips for spotting and avoiding voice scams. [Sitio Web]. [Consulta: 22 de enero de 2021]. Disponible en: https://us.norton.com/internetsecurity-online-scams-vishing.html

[13] TECHTARGET. Whaling attack (whaling phishing). [Sitio Web]. [Consulta: 20 de enero de 2021]. Disponible en: https://searchsecurity.techtarget.com/definition/whaling

RESUMEN

Para lograr analizar el impacto de los ataques de ingeniería social en Colombia desde el año 2016 hasta el año 2019, se debe realizar una breve descripción de la terminología relacionada a la Ingeniera social, normativa, legislación y conceptos; logrando concluir cuáles son las técnicas de ingeniería social más utilizadas y que afectan a la población colombiana. Otro aspecto importante es identificar si existen estrategias o campañas por parte de las entidades del estado, para contribuir a mitigar la ocurrencia de incidentes relacionados o producidos.

Se puede lograr que la ciudadanía, los entes gubernamentales y las empresas, identifiquen el tema como una problemática socioeconómica, que puede afectar desde su entorno familiar y laboral de las personas, o la empresa en general, y así se logre implementar a nivel educativo términos fundamentales de ingeniería social y poder mitigar la brecha de la inseguridad por la ejecución de dichas técnicas, aprovechando las falencias del ser humano, que por naturaleza es confiado.

El propósito fundamental es obtener un conjunto de buenas prácticas y recomendaciones para que las personas no se vean afectadas por ataques de ingeniería social, para que posteriormente las organizaciones las puedan utilizar para realizar la concienciación del personal y como estrategia de prevención.

Palabras clave: Engaño, estafa, ataque, ciber-delincuente, *Phishing*.

ABSTRACT

In order to analyze the impact of social engineering attacks in Colombia from 2016 to 2019, a brief description of the terminology related to social engineering, regulations, legislation and concepts should be made; managing to conclude which are the most used social engineering techniques that affect the Colombian population. Another important aspect is to identify if there are strategies or campaigns on the part of the state entities, to help mitigate the occurrence of related or produced incidents.

It can be achieved that citizens, government entities and companies identify the issue as a socio-economic problem, which can affect people's family and work environment, or the company in general, and thus achieve implementation at the level educational fundamental terms of social engineering and to mitigate the gap of insecurity by the execution of these techniques, taking advantage of the shortcomings of the human being, who by nature is trusted.

The fundamental purpose is to obtain a set of good practices and recommendations so that people are not affected by social engineering attacks, so that organizations can later use them to raise awareness and as a prevention strategy.

Key words: Hoax, Scam, Attack, Cyber-criminal, Phishing.

1. INTRODUCCIÓN

Con el transcurso del tiempo, empresas, trabajadores y consumidores no logran dimensionar el valor que representan los activos de información, y se exponen a una perdida innecesaria de datos o de dinero. Los ciber delincuentes son conscientes de esta situación y mediante diversas técnicas buscan engañar a los usuarios para obtener un beneficio, generalmente económico.

Por esta razón se analiza el impacto de los ataques de ingeniería social en Colombia desde el año 2016, para lograr identificar cuáles delitos informáticos relacionados a la ingeniería social son los que más se producen en el país. Otro aspecto por verificar es la evolución que han tenido dichos ataques, puesto que a medida que mejora la tecnología y las medidas de protección, también las técnicas utilizadas por los atacantes se fortalecen.

Para responder a la necesidad de protección ante la ingeniería social que exige la sociedad, es necesario hacer la revisión de las estrategias diseñadas para este fin por parte de las entidades del estado o entidades privadas. Esto permite conocer qué aspectos contribuyen a mitigar de alguna manera este riesgo.

La información de personas o empresas se encuentra pública en sitios de internet, ya que no se cuenta con una cultura de seguridad de la información y no se presta atención a lo que se expone en la red. Esta información es la que más adelante les permite a los atacantes construir su estrategia de ataque y de alguna manera ganar la confianza de las víctimas, para finalmente acceder a los datos confidenciales o simplemente engañar para obtener beneficio económico.

El presente trabajo es importante ya que se obtiene un conjunto de buenas prácticas y recomendaciones mediante las cuales es posible contribuir para la concienciación en seguridad de la información que corresponda con gran iniciativa a lo para la

elaboración de una guía que les permita a las personas tomar medidas de protección frente a este tipo de ataques. Se puede tener innumerables tipos de contraseñas, protección física o lógica, pero cuando el activo de la información se encuentra bajo en manejo d un ser humano, es posible ser vulnerado con más facilidad analizando el origen y la evolución de los ataques de la ingeniería social.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES DEL PROBLEMA

La ingeniería social supone una práctica en términos de la seguridad informática, como un conjunto de técnicas empleadas para obtener información confidencial, mediante la manipulación de la víctima, generalmente lo que el atacante busca es obtener algún tipo de beneficio, ya sea económico o la obtención de datos personales, credenciales de acceso o números de cuentas.

Una de las estafas más conocidas es el famoso timo 419 (carta nigeriana), que según la tesis Fraudes en Internet de Dinca[14], es uno de los más antiguos, y tomó ese nombre porque viola el artículo 419 del código penal de Nigeria. Este fraude consiste en prometer a la víctima parte de una enorme fortuna para hacer efectiva la transferencia del dinero, se solicitan datos personales y número de cuenta bancaria. Un aspecto importante es que la persona que supuestamente será beneficiada debe cubrir unos gastos que se generan por la transferencia internacional y otros trámites requeridos para completar el traspaso de los fondos.

Con la masificación de las tecnologías y el acceso a internet los delincuentes encontraron un campo de acción más amplio para llevar a cabo las estafas y engaños, en el Boletín de Información, número 324 de Sánchez Medero[15] Delitos en internet: clases de fraudes y estafas y las medidas para prevenirlos, menciona que a través del *mail spoofing*, se logran obtener números de tarjetas de crédito, esta técnica consta de la suplantación por medio de correo electrónico de una entidad legitima, en este caso de un banco.

[14] DINCA, Claudia Florentina. Fraudes en Internet [en línea]. Trabajo de grado. Universitat Jaume I. 2016. [Consultado 22 abril 2020]. Disponible en http://repositori.uji.es/xmlui/bitstream/handle/10234/161252/TFG_2016_DincaClaudia.pdf?sequence=1

[15] Delitos en Internet: Clases de fraudes y estafas y las medidas para prevenirlos [en línea]. Madrid: Universidad Complutense de Madrid, 2012. [Fecha de consulta: 22 abril 2020]. Disponible en internet: https://dialnet.unirioja.es/descarga/articulo/4198948.pdf

En el artículo, Estafas informáticas a través de Internet: acerca de la imputación penal del "*Phishing*" y el "*pharming*" de Oxman[16], se realiza una aproximación a nivel legal de las consecuencias que acarrean para los delincuentes la práctica de estos dos tipos de fraudes informáticos. No obstante, existe normativa en los países que condenan estos delitos, pero aun así se siguen cometiendo, ya que muchas veces las victimas prefieren no denunciar.

En Colombia, la situación en cuanto a los ataques de ingeniería social va en aumento, de acuerdo con el informe publicado por la Cámara Colombiana de Informática y Telecomunicaciones[17], Tendencias cibercrimen Colombia 2019-2020, los incidentes que más se reportan en el país son: *Phishing* 42%, suplantación de identidad 28%, envío de *malware* 14% y los fraudes 16%.

Según este informe, la tendencia para el año 2020 en Colombia es que este tipo de ataques de ingeniería social aumenten, haciendo uso de BEC "*Business Email Compromise*" basado en *Deepfake* (técnica de inteligencia artificial que permite la edición de videos y audios falsos de personas que hacen pasar por reales), *Botnets* para difusión de correos extorsivos, uso de perfiles falsos para difundir *malware* y tráfico de datos robados en *Darknet*.

1.2 FORMULACIÓN DEL PROBLEMA

¿Cuál ha sido el impacto de los ataques de ingeniería social en Colombia desde el año 2016 hasta el año 2019?

[16] Revista de Derecho [en línea]. Valparaíso: Pontificia Universidad Católica de Valparaíso, 2016. [Fecha de consulta: 22 abril 2020]. Disponible en internet: https://scielo.conicyt.cl/pdf/rdpucv/n41/a07.pdf

[17] CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias cibercrimen Colombia 2019-2020. Bogotá D.C. 2019. P.6.

2. JUSTIFICACIÓN

Aunque la ingeniería social y los ataques relacionados no son algo novedoso, desde hace muchos años se ha venido hablando del tema y se ha producido información al respecto, pero al observar un panorama de los ciber delitos en el mundo se observa cómo ataques de ingeniería social se ubican dentro de los primeros lugares, y a medida que avanza la tecnología e internet, estos ataques evolucionan de la misma manera encontrando técnicas cada vez más sofisticadas.

En el trabajo de grado titulado Estudio de metodologías de Ingeniería Social, se define como un "conjunto de técnicas o estrategias sociales que se utilizan de manera predeterminada por un usuario para obtener algún tipo de ventaja respecto a otros"[18]. Esto implica que aún no existe ningún sistema que este en capacidad de prevenir estos ataques.

Para el año 2016, en Colombia el crecimiento de los ataques de ingeniería social fue considerable, esto se reporta en el informe, Amenazas del cibercrimen en Colombia 2016-2017 de la Policía Nacional, donde se evidencia que hubo un incremento del 114% de ataques de *malware* con respecto al año 2015, el hurto por medios informáticos y semejantes represento el 68% de los casos reportados, seguido del acceso abusivo a un sistema informático con 13% y violación de datos personales con 12%[19].

El informe Balance cibercrimen en Colombia 2017 de la Policía Nacional, hace un resumen del año 2017 en cuanto a ciberdelitos en Colombia, lo cual arroja resultados poco esperanzadores ya que se incrementan los delitos y aparecen

[18] SERRATO BERENGUER, David. Estudio de metodologías de Ingeniería Social [en línea] Trabajo fin de Máster. Universitat Oberta de Catalunya, 2018. [Consultado 14 abril 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf
[19] POLICÍA NACIONAL DE COLOMBIA. Amenazas del cibercrimen en Colombia 2016-2017. Bogotá D.C.: Ministerio de Defensa Nacional, 2017. P.10.

nuevas técnicas para engañar a los ciudadanos, el 60% de las estafas se realizaron por compra o venta en línea, *Vishing* estafas por llamadas telefónicas 16%, engaños a través de mensajes de texto (*Smishing*) 13%, estafas asociadas a cartas nigerianas 8% y para cerrar ofertas fraudulentas con un 2%[20].

La problemática que golpea a la población es evidente, ya que los delincuentes pasan al mundo digital para cometer las actividades ilícitas, y es allí donde logran captar bastantes víctimas, en el caso de un *Phishing* en cuestión de minutos el atacante puede enviar el señuelo a miles de personas, y solamente tiene que esperar que empiecen a morder el anzuelo.

Una implicación adicional de la ingeniería social es que también se utilizan estas técnicas para realizar la distribución de virus, gusanos, *spyware*, *ransomware* y otros programas maliciosos usados para obtener información confidencial[21], así lo manifiesta el Ministerio de tecnologías de la información y las comunicaciones de Colombia, en la "Guía para la implementación de seguridad de la información en una MIPYME".

[20] POLICÍA NACIONAL DE COLOMBIA. Balance cibercrimen en Colombia 2017. Bogotá D.C.: Ministerio de Defensa Nacional, 2017. P.6.
[21] MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Guía para la implementación de seguridad de la información en una MIPYME. Bogotá D.C. 2016. p.15.

3. OBJETIVOS

3.1 OBJETIVOS GENERAL

Analizar el impacto de los ataques de ingeniería social en Colombia desde el año 2016, para la elaboración de una guía que les permita a las personas tomar medidas de protección frente a este tipo de ataques.

3.2 OBJETIVOS ESPECÍFICOS

- Definir el origen y la evolución de los ataques de ingeniería social.
- Determinar cuáles de los ataques de ingeniería social son los más utilizados en Colombia para engañar a las personas.
- Identificar qué estrategias se han propuesto por parte de las entidades del estado colombiano para la mitigación de los ataques de ingeniería social.
- Sugerir un conjunto de buenas prácticas y recomendaciones para que las personas no se vean afectadas por ataques de ingeniería social.

4. MARCO REFERNCIAL

4.1 MARCO TEÓRICO

Los ataques de ingeniería social se han encargado de comprobar que el eslabón más débil de la cadena de la seguridad informática es el ser humano, ya que continúan presentándose incidentes de ciberseguridad en donde el atacante obtiene credenciales de acceso o información sensible, gracias a la manipulación de un usuario. *Kevin Mitnik*, en su libro “El arte del engaño”, explica cómo logró obtener contraseñas o información sensible solamente fingiendo ser otra persona, esto a través de “un tipo de ataque contra el elemento humano durante el cual el atacante induce a la víctima a divulgar información o realizar acciones que no deberían” [22].

Uno de los activos con mayor valor para las organizaciones es la información que maneja. Dicha información es todo el conjunto de datos que proporciona sentido a una organización, datos que definen procesos, datos que intervienen en procedimientos y en caso de no tomar las medidas suficientes para protegerlos, serán datos que caerán en manos equivocadas.

Por otra parte, haciendo más extenso el concepto de seguridad en lo referente a las telecomunicaciones y la informática, es posible encontrar dos diferentes enfoques: seguridad de la información y seguridad informática. En primera medida, la seguridad de la información se constituye como un conjunto de medidas y procedimientos, de tipo humano y técnico cuyo objetivo es proteger la integridad, confidencialidad y disponibilidad de la información. Esto también es conocido como la tríada de la CIA, la cual se refiere a un modelo de seguridad de la información

[22] NOHLBERG, Marcus, Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks. Estocolmo. Universitetsservice US-AB. 2018. p.59. ISBN 978-91-7155-786-5

formado por tres componentes principales (Disponibilidad, Integridad, Confidencialidad), tal y como se puede evidenciar en la siguiente Figura:

Figura 1. Principios de la seguridad de la información.

Fuente: INCIBE. ¿Sabes qué es el Día Internacional de la Seguridad de la Información? [En línea]. Madrid.: Instituto Nacional de Ciberseguridad. 2019. (Recuperado en 16 mayo 2020) Disponible en: https://www.incibe.es/protege-tu-empresa/blog/sabes-el-dia-internacional-seguridad-informacion

De acuerdo con la definición anterior, el concepto es amplio porque reúne medidas de seguridad que impactan sobre la información sin importar su tipo; es decir, es independiente al medio de almacenamiento o la manera en la que es transmitida.

Por otra parte, la seguridad informática es una rama de la seguridad de la información cuyo objetivo es proteger toda aquella información que se gestiona a través de una infraestructura tecnológica, sistemas de información y telecomunicaciones. Esta protección va orientada a lo que se quiere proteger y al momento en el que se realiza la protección.

En función de lo que la organización quiere proteger:

- Seguridad física: protección física y del entorno (incendios, robos, inundaciones, etc.)
- Seguridad lógica: mecanismos de protección que se aplican sobre la parte lógica del sistema informático.

En función del momento en el que la organización efectúa la protección:

- Seguridad activa: tipo de seguridad que se encargada de prevenir, detectar y evitar incidentes que afectan a los sistemas informáticos.
- Seguridad pasiva: técnicas y procedimientos que se llevan a cabo para hacer que las consecuencias del incidente sean mínimas.

La mayoría de los profesionales de la seguridad informática están familiarizados con la ingeniería social y sus peligros. Pero hay que tener en cuenta que la ingeniería social puede tener diferentes definiciones, esto dependiendo del contexto. Para el desarrollo del presente documento la definición más aproximada y concisa es la propuesta por Alexander: "La ingeniería social es un vector de ataque que depende en gran medida de la interacción humana y a menudo implica engañar a las personas para que rompan los procedimientos normales de seguridad"[23].

Básicamente, para que un ataque logre tener el éxito y el impacto esperado, se debe engañar al usuario del sistema o persona, para este fin los atacantes han encontrado diferentes técnicas y métodos, los cuales a través del tiempo se han vuelto más sofisticados y con un nivel mayor de complejidad, esto asegura en cierta medida que para la víctima sea complicado evadir un ataque de esta naturaleza y por este motivo los ciber criminales encuentran en la ingeniería social un mecanismo efectivo para penetrar en las organizaciones, haciendo uso de:

[23] Methods for Understanding and Reducing Social Engineering Attacks [en Línea]. Boston: SANS Institute Information Security Reading Room, 2016. [Fecha de consulta: 14 mayo 2020]. Disponible en: https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972

4.1.1 *Phishing.* En el paper “Qué es el *Phishing* y cómo protegerse”, El *Phishing* se constituye como una de las modalidades de estafa preferida por los atacantes, con el fin de conseguir datos del usuario como su número de tarjeta de crédito, o cualquier información que posteriormente pueda ser utilizada de forma fraudulenta[24].

A manera de ejemplo, se presenta a continuación la figura 2 donde se puede apreciar un ataque de este tipo:

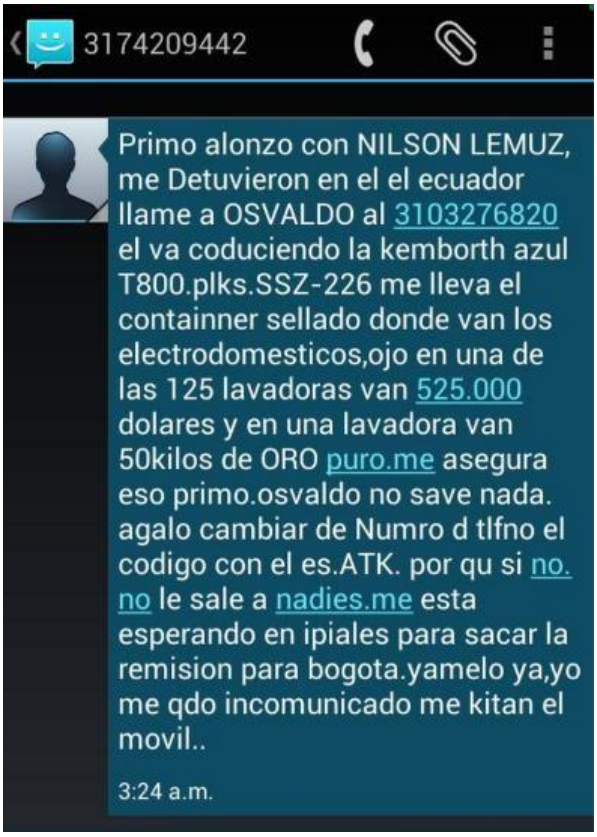
Figura 2. *Phishing* entidad bancaria.

Fuente: CAI VIRTUAL. Mural del ciber crimen. [En línea]. Bogotá D.C.: Policía Nacional de Colombia. 2017. (Recuperado en 16 mayo 2020) Disponible en: https://caivirtual.policia.gov.co/mural-cibercrimen/phishing

[24] ACENS TECHNOLOGIES. Qué es el *Phishing* y cómo protegerse. [Sitio web]. Madrid: Telefónica. [Consulta: 15 de abril 2020]. Disponible en: https://www.acens.com/wp-content/images/2014/10/wp-phising-acens.pdf

4.1.2 *Smishing*. Según el artículo científico “Seguridad por capas frenar ataques de *Smishing*” define a este término como una combinación de la palabra “*Phishing*” y “SMS”. Es un nuevo tipo de técnica o variante del *Phishing* que tiene como propósito robar la información de un usuario, mediante el uso del servicio de mensajería de texto (SMS) de un teléfono móvil[25]. Como se puede evidenciar en la figura 3 se tiene un ejemplo de esta modalidad:

Figura 3. *Smishing* ejemplo de estafa.



Fuente: CAI VIRTUAL. Mural del ciber crimen. [En línea]. Bogotá D.C.: Policía Nacional de Colombia. 2017. (Recuperado en 16 mayo 2020) Disponible en: https://caivirtual.policia.gov.co/mural-cibercrimen/smishing

[25] MARTÍNEZ SANTANDER, Carlos José. et al. Seguridad por capas frenar ataques de *Smishing*. Dominio de las ciencias [en línea] Manta - Manabí (Ecuador): Polo de Capacitación, Investigación y Publicación (POCAIP) 01 enero 2018, vol. 4, nro 1. [Consultado 6 abril 2020]. ISSN 2477-8818. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6255067.pdf

4.1.3 *Vishing.* (combinación de palabras ‘voz’ y ‘*Phishing*’) es un fraude telefónico en el que los estafadores intentan engañar a la víctima para que divulgue información personal, financiera o de seguridad, o que transfiera dinero [26], esta definición la presenta Europol en el documento titulado “Fraude del CEO”. En la ilustración se representa un ataque de este tipo.

Figura 4. Ilustración *Vishing*.

Fuente: IT CONNECT. *Vishing*: Group-IB deja al descubierto a peligrosa banda. [En línea]. Buenos Aires.: IT Connect. 2019. (Recuperado en 16 mayo 2020) Disponible en: https://itconnect.lat/portal/2019/02/15/vishing-0001/

4.1.4 *Impersonation*. Los ataques de suplantación de identidad pueden ser particularmente perjudiciales para la reputación en línea de la víctima. A medida que los motores de búsqueda agregan cada vez más los datos en línea de las personas y utilizado para una variedad de propósitos, incluida la evaluación de su idoneidad para el empleo, los ataques de suplantación, particularmente aquellos que no se detectan, pueden tener serios efectos adversos consecuencias para las víctimas, incluso en el mundo fuera de línea[27], así describen este ataque en el artículo “*Exposing Impersonation Attacks in Online Social Networks*”.

[26] EUROPOL. Fraude del CEO. [Sitio web]. The Hague: EUROPOL. [Consulta: 8 de abril 2020]. Disponible en: https://www.europol.europa.eu/sites/default/files/documents/colombia_1.pdf

[27] GOGA, Oana; VENKATADRI, Giridhari y GUMMADI, Krishna P. Exposing Impersonation Attacks in Online Social Networks. [En línea]. 2016, [Consultado 1 de mayo 2020]. Disponible en: https://lig-membres.imag.fr/gogao/papers/impers_cosn14.pdf

Actualmente para cualquier persona es común el uso de celular y equipos de cómputo, por este motivo es importante conocer y estar alerta sobre los distintos tipos de amenazas cibernéticas. Claudia Castillo de BBVA, menciona que: “El ‘*phishing’*, ‘*vishing’* y ‘*smishing’* son algunos los fraudes electrónicos que utilizan los ciber delicuentes para robar datos privados, pero mediante información y prevención se pueden evitar”[28].

Al tener las personas acceso con mayor facilidad a las tecnologías y dispositivos móviles, se facilita la actividad de los ciberdelincuentes ya que lanzan muchos ataques de este tipo a diario y la cantidad de víctimas potenciales es alto. Por esta razón los actores maliciosos continúan perfeccionando estas técnicas para conseguir una tasa de efectividad mayor.

4.2 MARCO CONCEPTUAL

La ingeniería social, según *Thomas Douglas*, investigador de la Universidad de Minnesota este término ha sido utilizado entre *crackers* y samurái para técnicas de *cracking* que dependen de debilidades en el factor humano, más que del *software*; cuyo objetivo es engañar a las personas para que revelen contraseñas u otra información que comprometa la seguridad de un sistema objetivo. Las estafas clásicas incluyen llamar a una marca que tiene la información requerida y hacerse pasar por un técnico de servicio de campo o un compañero de trabajo con un problema de acceso urgente.

Para enmarcar la ingeniería social dentro de la seguridad de la información se debe hacer una aproximación más detallada del término, para así comprender la importancia de no ser víctima de un ataque que utilice metodologías asociadas, lo

[28] BBVA. 'Phishing', 'vishing', 'smishing', ¿qué son y cómo protegerse de estas amenazas? [Sitio web]. Madrid.: Castillo, Claudia. [Consulta: 15 de mayo 2020]. Disponible en: https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

cual es un aspecto clave para determinar los conceptos de forma más acertada y ajustada.

En el artículo “Ingeniería Social: El Ataque Silencioso”, se explica que el fin del atacante que hace uso de la ingeniería social es explotar al eslabón más débil de la organización, el usuario. Dependiendo de su osadía, habilidades y conocimientos, el atacante puede utilizar herramientas tecnológicas, incluso encuentros cara a cara para obtener la información que necesita[29]. Es relevante reconocer que, no solamente el usuario final de los sistemas de información está expuesto a sufrir un ataque de Ingeniería Social; el personal de seguridad informática también está expuesto y es igual de vulnerable, situación que pudo ser comprobada por el “Experimento *Robin Sage*”. En este experimento se creó un perfil falso en las redes sociales *twitter*, *LinkedIn* y *facebook, Robin Sage*, 25 años, Analista de seguridad en la Armada de los EE.UU. Graduada en el MIT 10 años de experiencia en seguridad, transcurridos 28 días logra conseguir: 300 contactos, acceso a datos militares confidenciales, 2 ofertas de trabajo (una de ellas de *Google*). La identidad, por supuesto, era falsa, la foto fue extraída de un sitio web de pornografía, esto en la red ayudó a generar la confianza[30].

Para que un ataque de ingeniería social impacte de la manera esperada en la víctima, es necesario que se recopile cierta información previamente (a través de internet o presencialmente), lo cual ayuda a confundir o distraer al usuario, ya que se da una falsa sensación de seguridad cuando se proporcionan datos que supuestamente solo podrían saber entidades o personas que tienen alguna relación

[29] LÓPEZ GRANDE, Carlos Edgardo y SALVADOR GUADRÓN, Ricardo. Ingeniería Social: El Ataque Silencioso [en línea]. 2015, enero –diciembre, vol.7, nro.1. [Consultado 02 de mayo 2020]. ISSN 2072-568X. disponible en: http://www.redicces.org.sv/jspui/bitstream/10972/2910/1/Articulo6.pdf

[30] AENOR. Seguridad en Sistemas de Información Un recorrido a vista de pájaro. [Sitio web]. Ciudad Real. [Consulta: 1 de mayo 2020]. Disponible en: https://ruidera.uclm.es/xmlui/bitstream/handle/10578/2302/Seguridad%20en%20Sistemas%20de%20Informaci%C3%B3n%20ESI%202012-0.4.pdf?sequence=1&isAllowed=y

directa. Por este motivo es que generalmente se suplantan organizaciones o empresas de renombre. Tal y como se evidencia en el siguiente Cuadro:

Cuadro1. Amenazas y vulnerabilidades

	2013	2014	2015	2016
Vulnerabilidades				
Empleados descuidados o desinformados	53%	57%	44%	55%
Controles de seguridad o arquitectura de información desactualizados	51%	52%	34%	48%
Acceso no autorizado	34%	34%	32%	54%
Amenazas				
Malware	41%	34%	43%	52%
Suplantación de identidad (*Phishing*)	39%	39%	44%	51%
Ataques cibernéticos para robar información financiera	46%	51%	33%	45%
Ataques cibernéticos para robar *IPs* o datos	41%	44%	30%	42%
Ataque internos	28%	31%	27%	33%

Fuente: LAMPADIA. Fortaleciendo las capacidades de seguridad cibernética.

El Instituto Nacional de Ciberseguridad de España, en el artículo "*OSINT* - La información es poder" (La Inteligencia de fuentes abiertas – *OSINT*) es el proceso de recopilar datos disponibles de fuentes abiertas públicas para su uso en labores de inteligencia. En el contexto de las agencias de inteligencia, el término "abierto" se refiere a fuentes que están disponibles para el público en general en contraposición a fuentes cerradas/clasificadas o clandestinas[31]. Por otra parte, el artículo "Ingeniería social: ¿Se puede *hackear* a una persona?", establece que independientemente de cómo se obtenga la información mediante OSINT, es

[31] INCIBE. OSINT - La información es poder. [Sitio web]. Madrid. [Consulta: 30 de abril 2020]. Disponible en: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

necesario tener una idea clara sobre lo que se busca[32]. A primera vista, puede parecer algo sencillo, pero no lo es. Inicialmente se piensa en obtener toda la información sobre el objetivo, pero cada tipo de información tiene diferente valor y el valor puede cambiar con el tipo de ataque que se esté buscando ejecutar.

Existen técnicas que han evolucionado, de tal forma que se presentan como ataques más precisos y que casi siempre logran su cometido. Los ciber criminales buscan que el impacto sea alto y se dirigen a organizaciones que manejan información más relevante y valiosa que un usuario convencional.

Una característica de la ingeniería social es que evoluciona de acuerdo con las exigencias del entorno y las técnicas asociadas también adquieren dimensiones diferentes, logrando un nivel de efectividad que permite vulnerar incluso a personal con conocimientos técnicos o competencias en seguridad informática, algunas de las modalidades más usadas actualmente son:

4.2.1 *Spear phishing*. Es usado por atacantes más sofisticados que delimitan su objetivo y aumentan la precisión de los mensajes, haciendo atractivo del mensaje y de una aparente legitimidad. De acuerdo con *CERT-UK*, en *An introduction to social engineering*: “Si bien un ataque dirigido de este tipo disminuye el número de víctimas potenciales, también es probable que resulte en un mayor beneficio para el atacante”[33].

La mayoría de los correos electrónicos que se envían de esta manera parecen legítimos y son extremadamente difícil de identificar como malicioso.

[32] POLICÍA MUNICIPAL DE MADRID. Ingeniería social: ¿Se puede *hackear* a una persona? [Sitio web]. Madrid. [Consulta: 1 de mayo 2020]. Disponible en: https://cppm.es/wp-content/uploads/2019/03/ingenieria-social-se-puede-hackear-a-una-persona-abr2019.pdf

[33] CERT-UK. An introduction to social engineering. [Sitio web]. Londres. [Consulta: 14 de mayo 2020]. Disponible en: https://www.oodaloop.com/wp-content/uploads/2015/02/UKCERT-SocialEngineering.pdf

4.2.2 *Baiting.* Es muy similar a un troyano, utiliza un medio físico, y hace uso de la curiosidad o avaricia de la víctima. Se asemeja a un ataque de *phishing*. Sin embargo, “lo que lo hace diferente de otros tipos de ataques de ingeniería social es el ofrecimiento de un artículo u objeto que los piratas informáticos usan para atraer a sus víctimas”[34]. Los *baiters* (así son llamados estos atacantes) en ocasiones utilizan música o descargas gratuitas de películas, si ofrecen credenciales a una determinada página o sitio web.

4.2.3 *Watering hole attack.* “Este ataque busca comprometer a un grupo específico de usuarios finales al infectar sitios web que los miembros del grupo visitan”[35]. El objetivo es infectar la máquina de un usuario y obtener acceso a la red en el lugar de trabajo del objetivo.

4.2.4 *Quid pro quo.* Es un ataque que promete la obtención de beneficios a cambio de información[36]; el beneficio que normalmente se ofrece es un servicio, en el caso del *baiting* se ofrece un bien a cambio. Se puede considerar una solicitud de información suya o de su organización a cambio de algún tipo de compensación, que puede ser servicio técnico o servicios profesionales. Una de las primeras descripciones sistemáticas del proceso de explotación de la ingeniería social como un vector de ataque fue dado por *Kevin Mitnick*[37]. El proceso que propone tiene cuatro fases:

[34] MAILFENCE. Ingeniería Social: ¿qué es el Baiting («cebar», o «poner carnada»)? [Sitio web]. [Consulta: 10 de mayo 2020]. Disponible en: https://blog.mailfence.com/es/que-es-baiting-ingenieria-social/

[35] TECHTARGET. Watering hole attack. [Sitio web]. San Francisco. [Consulta: 05 de mayo 2020]. Disponible en: https://searchsecurity.techtarget.com/definition/watering-hole-attack

[36] MAILFENCE. Ingeniería Social: ataques de Quid pro Quo. [Sitio web]. [Consulta: 10 de mayo 2020]. Disponible en: https://blog.mailfence.com/es/ataques-de-quid-pro-quo/

[37] MITNIK, Kevin. The Art of Deception. Indianapolis: WILEY Publishing, Inc, 2001. p.350. ISBN 0-471-23712-4

• Investigación: Se refiere al proceso de recopilar tanta información como sea posible sobre el objetivo. Esta información se utiliza en fases posteriores y es de importancia crítica para realizar los ataques dirigidos.

• Desarrollo de *Rapport* and *Trust*: En esta fase se hace uso de varias técnicas para lograr que la víctima confíe en el atacante. La información recopilada en la fase anterior, a menudo se usa para ese propósito.

• Explotación de la confianza: En la fase de "explotación" de un ataque de ingeniería social, el atacante logra una ganancia medible en información o privilegios.

• Utilice la información: En la fase final del ciclo hace referencia a "cobrar" las ganancias obtenidas en la fase anterior. Como lo insinúa el término "Ciclo de ataque", esta fase puede pasar nuevamente a otra fase de investigación, completando así la naturaleza cíclica del proceso. Esta transición es la ingeniería social.

4.3 MARCO LEGAL

El estado colombiano, a través del Congreso de la Republica, para dar respuesta a una creciente problemática y el riesgo que representan los delitos informáticos, promulgo la ley denominada: “De la protección de la información y de los datos”. Ley 1273 de 2009. "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones"[38].

[38] COLOMBIA. CONGRESO DE LA REPUBLICA, Ley 1273 (5, enero, 2009). "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos". Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1-4.

En lo contemplado por esta ley, se encuentran tres artículos que resultan relevantes para tipificar y establecer la conducta delictiva de los ataques de ingeniería social:

Artículo 269A. ACCESO ABUSIVO A UN SISTEMA INFORMÁTICO.

Artículo 269G. SUPLANTACIÓN DE SITIOS WEB PARA CAPTURAR DATOS PERSONALES.

Artículo 269J: TRANSFERENCIA NO CONSENTIDA DE ACTIVOS.

Esta serie de conductas delictivas relacionadas con el manejo de datos personales, hacen que la ley 1273 sea de importancia para que las empresas y organizaciones, les permite blindarse de forma jurídica para evitar que se incurra en alguno de los tipos penales allí mencionados. Los avances tecnológicos y el uso de estos para obtener de manera ilícita el patrimonio de terceros a través de la clonación de tarjetas de crédito o débito, vulneración y/o alteración de sistemas de cómputo para adquirir servicios, realizar transferencias electrónicas de fondos manipulando programas y afectación a cajeros automáticos. Estas son conductas que se han vuelto usuales en cualquier parte del mundo[39].

La Policía Nacional de Colombia, tiene como línea base para el tratamiento de delitos informáticos, el CÓDIGO PENAL COLOMBIANO LEY 599 DE 2000. [40] A través de otras normas en la legislación nacional el Gobierno Nacional realiza una aproximación al tratamiento de delitos informáticos y sus penalizaciones, entre ellas están:

[39] DELTA ASESORES. Ley de Delitos Informáticos en Colombia. [Sitio web]. Bogotá. [Consulta: 5 de mayo 2020]. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

[40] COLOMBIA. CONGRESO DE LA REPUBLICA, Ley 599 (24, julio, 2000) Código Penal Colombiano. Diario Oficial. Bogotá, D.C. 2000. No. 44.097. p 1-428.

• Ley estatutaria 1266 de 2008, “por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales”[41].

• Ley 1341 de 2009, “por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las TIC, también con esta ley se crea la Agencia Nacional de Espectro”[42].

En el año 2018, el Congreso de la Republica de Colombia reglamenta la Ley 1928 de 2018, en la cual se realiza la aprobación del “Convenio sobre la ciberdelincuencia”[43], el cual el primer tratado de orden internacional que tiene como objetivo hacer frente a los delitos informáticos y a los delitos cometidos en Internet. Adoptado el 23 de noviembre de 2001, en BUDAPEST[44]. También conocido como Convenio de Budapest sobre ciberdelincuencia o simplemente Convenio de Budapest. Fue elaborado por el Consejo de Europa en Estrasburgo, con participación de manera activa de Canadá, Japón y China como entes observadores.

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

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

[43] COLOMBIA. CONGRESO DE LA REPUBLICA, Ley 1928. (24, julio, 2018). Por medio de la cual se aprueba el «CONVENIO SOBRE LA CIBERDELINCUENCIA», Adoptado el 23 de noviembre de 2001, en Budapest. Diario Oficial. Bogotá, D.C., 2018. no. 50.664. p.1-49.

[44] HUNGRIA. CONSEJO DE EUROPA. (23, noviembre, 2001). Convenio sobre la ciberdelincuencia. Serie de tratados europeos. Budapest, Hungría. 2001. No. 185. p. 1-26.

4.3.1 CONPES 3701. Lineamientos de política para ciberseguridad y ciberdefensa. Este documento pretende generar: “lineamientos de política en ciberseguridad y ciberdefensa orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país”[45]. Adicionalmente, recopila los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.

4.3.2 CONPES 3854. Política nacional de seguridad digital. En el marco de la ejecución del Documento CONPES 3854 Política Nacional de Seguridad Digital, “se han realizado reuniones periódicas de coordinación y seguimiento, en las cuales se ha evidenciado la pertinencia de que la Dirección de Seguridad de la Presidencia de la República asuma las actividades de coordinación y articulación de las políticas de seguridad en el país, de conformidad con las funciones propias de la citada dependencia”[46]. La Presidencia de la República es el máximo órgano ejecutivo y su Dirección de Seguridad se encarga de la coordinación y concertación de políticas y estrategias de seguridad nacional y, además, hace el seguimiento a su cumplimiento.

[45] COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3701. (14, Julio, 2011). Lineamientos de política para ciberseguridad y ciberdefensa. Bogotá D.C. 2009. p. 1-43.
[46] COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3854. (7, marzo, 2017). Política nacional de seguridad digital. Bogotá D.C. 2017. p. 1-2.

5. DESARROLLO DE LOS OBJETIVOS

En este apartado se va a describir de una mejor manera la ingeniería social, orígenes, evolución y demás factores importantes para el desarrollo del proyecto.

5.1 ORIGEN Y EVOLUCION DE LOS ATAQUES DE INGENIERIA SOCIAL

"Es bien sabido por los expertos en seguridad informática que ninguna información es irrelevante"[47]. Esto aplica cuando se trata de recopilación de información, incluso el más mínimo detalle puede conducir a una violación exitosa de la ingeniería social. Muchos usuarios tienen la errónea percepción de que sus datos o información no le interesan a nadie, por esta razón nunca toman las medidas suficientes para protegerse.

La ingeniería social como ya se mencionó anteriormente se remonta al año 1894, lo cual hace que sea un tema muy conocido. No obstante, con la aparición de internet (*ARPANET*) y posteriormente en el año 1971 cuando es enviado el primer correo electrónico por *Ray Tomlinson*, empieza una nueva era en cuanto a las redes de computadores y la forma de acceder a la información.

En el año 1981 se realiza la definición formal del protocolo *TCP/IP* y de la palabra internet. Para el año 1989, había 100000 computadores conectados a *internet* y el constante crecimiento de la red se evidenció apenas tres años después, cuando se alcanza el millón de computadoras conectadas a *internet*.

Los primeros casos de *phishing* tal y como se conocen actualmente se produjeron en el año 1996 y eran dirigidos a usuarios de la empresa América *Online* (AOL).

[47] HADNAGY, Christopher y WILSON, Paul, Ingeniería social: El arte de la piratería humana. New York. John Wiley & Sons, Incorporated, 2010. p.40. ISBN 9780470639535

A partir de este punto la ingeniería social se ha convertido en una de las armas preferidas por los atacantes, ya que gracias a sus técnicas y métodos logran que los ataques tengan mayor efectividad y finalmente obtener el beneficio esperado. Para lograr entender de mejor manera los ataques de ingeniería social, se realiza una recopilación de las técnicas más relevantes y de las nuevas variaciones o evoluciones que han tenido a través de los años.

5.1.1 *Phishing* general. *Phishing* tradicional, *Bulk Phishing* o *Spray* and *pray*. En la actualidad, muchas de las campañas de *phishing* son planeadas, organizadas y ejecutadas por profesionales. Los atacantes han tecnificado el *phishing* e implementan kits preparados con plantillas, páginas *web* y mensajes de correo electrónico genéricos, además de otras herramientas que son necesarias para montar los ataques. En otras palabras, es la actividad dirigida a sustituir de forma fraudulenta la identidad de una persona o entidad con el objeto de adueñarse de forma indebida de datos confidenciales de acceso y contraseñas de los usuarios para, lograr deteriorar o desprestigiar su imagen o apropiarse de su patrimonio[48].

Las páginas *web* a menudo son réplicas exactas de las páginas que se están falsificando. Además, *Digicert* manifiesta que "los mensajes de *phishing* no solo están bien redactados, sino que incluyen toda una serie de mecanismos para evitar los filtros de *spam*"[49].No como sucedía anteriormente que los errores de ortografía o gramática alertaban al usuario.

5.1.2 *Vishing*. "La inteligencia artificial ya puede clonar nuestra voz a partir de una pequeña muestra de audio, lo que ha agudizado el ingenio de los que intentan

[48] BALBOA-ROMERO. Francisco José. Ransomware, hacking y phishing: conducta típica del delito de daños informáticos [en línea]. [Consulta: 22 de noviembre de 2020]. Disponible en: https://reunir.unir.net/bitstream/handle/123456789/6929/BALBOA%20ROMERO%2c%20FRANCISCO%20JOS%c3%89.pdf?sequence=1&isAllowed=y

[49] DIGICERT. Breve historia del phishing. [Sitio web]. Madrid. Digicert. [Consulta: 10 de mayo 2020]. Disponible en: https://www.websecurity.digicert.com/es/es/security-topics/brief-history-phishing-part-1

engañar con estafas por teléfono”[50]. También conocidos como *Deepfakes* de audio, mediante el cual a partir de grabaciones de voz es posible utilizar software como *Lyrebird* para generar una voz sintética y que al ser transmitida mediante una llamada telefónica es aún más difícil para la victima detectar el engaño.

5.1.3 *Smishing*. Al igual que los otros ataques el *smishing*, también se han tecnificado e implementado nuevos elementos con el propósito de ser cada vez más convincentes. *Colin Asher* de *AVG* resalta el hecho de que “las empresas legitimas utilizan un «*shortcode*» para enviar los mensajes de texto. Esto código es grupo pequeño de números que reemplazan a un número telefónico real, los estafadores usan números breves de similar estructura para su contenido”[51]. Y aún más dañino resulta el hecho de que, a veces, los mensajes fraudulentos pueden auto insertarse en un hilo de mensajes legítimos ya existente.

5.1.4 URL *Phishing*. Los atacantes en ocasiones buscan dirigir a la víctima a un sitio *web* malicioso, para lograr esto utilizan diferentes formas para que el usuario no logre identificar una URL real a una URL engañosa. Una de las técnicas más utilizadas para este propósito es la homografía, lo cual consiste en hacer uso de caracteres Unicode que visualmente sean semejantes, para demostrar mejor se usa, www.google.com y www.googIe.com visualmente son iguales, pero en el segundo caso en lugar de la letra l (ele) se utiliza la letra I (i) mayúscula.

Otra técnica es aprovechar los errores tipográficos, a lo que se conoce como *Typosquatting*. Para continuar con el mismo ejemplo puede ser www.google.com y www.ggogle.com incluso algunas compañías compran este tipo de dominios que puedan significar algún tipo de amenaza por su gran similitud.

[50] EL PAIS. Inteligencia artificial Llega el ‘vishing’: ¿hablas con tu madre o con una máquina que ha aprendido a imitarla? [Sitio web]. Madrid. Retina. [Consulta: 10 de mayo 2020]. Disponible en: https://retina.elpais.com/retina/2019/10/21/tendencias/1571641240_168585.html

[51] AVG Antivirus. Qué es el smishing y cómo evitarlo. [Sitio web]. Praga. Asher, Colin. [Consulta: 11 de mayo 2020]. Disponible en: https://www.avg.com/es/signal/what-is-smishing

5.1.5 *Whaling*. Es una combinación de fraude que se deriva del *phishing*; donde los ciber delincuentes apuntan a personas con cargos importantes, gran manejo de dinero y toma de decisiones en la compañía; el ataque va dirigido a una persona específicamente y haciendo uso de técnicas de ingeniera social persuaden para que se produzca una entrega de información confidencial.

5.1.6 *Business Email Compromise (BEC*) o estafas *Man-in-the-Email*. Con un *BEC*, un atacante utiliza sus conocimientos de la empresa, en lugar de usar un simple ataque de spam. “Nombres y direcciones de correo electrónico corporativos de empleados o clientes, así como las firmas actuales, hacen que un correo electrónico falso parezca auténtico”[52], según *Kreyenberg* son los aspectos clave para asegurar el éxito del ataque. Los ciberdelincuentes envían un mensaje de correo electrónico corto (sólo de texto) a determinado empleado. Utilizan una dirección de correo electrónico falsa similar a la del CEO, la de un cliente o de un empleado. El nombre se muestra exactamente cómo aparecería en el correo electrónico de la persona real. Esto dificulta la detección del fraude que hay detrás.

En la siguiente Figura se muestran las fases que componen a un ataque BEC, en donde el atacante inicialmente identifica el objetivo, recopila información y perfila a los empleados, después a través de técnicas de ingeniería social trata de engañar a los empleados, después de lograr el engaño solicita información o transferencia de activos y finalmente la victima accede a realizar la transferencia solicitada completando el ataque de manera éxitos.

52 HORNET SECURITY. Bussiness email compromise. [Sitio web]. Hannover.: Kreyenberg. Hannah. [Consulta: 16 mayo 2020]. Disponible en: https://www.hornetsecurity.com/es/seguridad-de-la-informacion/business-email-compromise-bec-la-amenaza-crece-rapidamente/

Figura 5. *BEC*.

Fuente: HORNET SECURITY. Bussiness email compromise. [En línea]. Hannover.: Kreyenberg. Hannah. 2019. (Recuperado en 16 mayo 2020) Disponible en: https://www.hornetsecurity.com/es/seguridad-de-la-informacion/business-email-compromise-bec-la-amenaza-crece-rapidamente/

5.1.7 *CEO Fraud*. Estrechamente relacionada con el ataque anterior, en esta estafa los ciber delincuentes falsifican o suplantan cuentas de correo electrónico corporativas y se hacen pasar por altos ejecutivos para tratar de engañar a un empleado de contabilidad, área financiera o recursos humanos para que ejecute transferencias electrónicas no autorizadas o envíe información fiscal confidencial.

5.1.8 *Spear Phishing*. Este ataque ya no es efectivo en volumen, sino que los ciber delincuentes apuntan a un objetivo definido, la campaña de *phishing* va dirigida hacia una persona por un interés concreto o como estrategia para llegar a otra persona y por esto se personalizan los envíos. Para que el engaño pueda efectuarse los atacantes recaban datos de la víctima. Consultan redes sociales, averiguan aspectos sobre su estilo de vida, rutinas o cosas que relacionadas a esta persona para hacerle creer que lo que le está llegando es real. Es una técnica más refinada pero que si funciona puede ser clave para alcanzar cualquier tipo de objetivo que se propongan.

El *spear phishing*, una estrategia común de ataque por correo electrónico que se dirige a individuos específicos, y se constituye como una de las principales causas de penetración de los sistemas en las organizaciones[53].

5.1.9 *Search Engine phishing*. El *phishing* en los motores de búsqueda se produce cuando la víctima realiza una búsqueda, puede encontrar ofertas o mensajes que la atraigan a visitar el sitio web. El proceso de búsqueda puede ser legítimo, pero el sitio web es falso y solo existe para robar la información personal de la persona. los delincuentes no se molestan en realizar el envío de correos electrónicos. “Por el contrario, construyen su propio sitio y ofrecen ofertas increíbles o productos baratos que puedan llamar la atención de la víctima. También consiguen que el sitio sea indexado por motores de búsqueda legítimos”[54].

Por regla general, los motores de búsqueda se financian con publicidad. Los motores de búsqueda devolverán páginas patrocinadas como resultado inicial de su búsqueda, luego devolverán resultados que parecen estar más estrechamente asociados con el tema de búsqueda o con palabras clave de la búsqueda. “Existe una serie de riesgos con los motores de búsqueda, siendo el principal confiar en que siempre el motor de búsqueda devolverá resultados genuinos y seguros”[55].

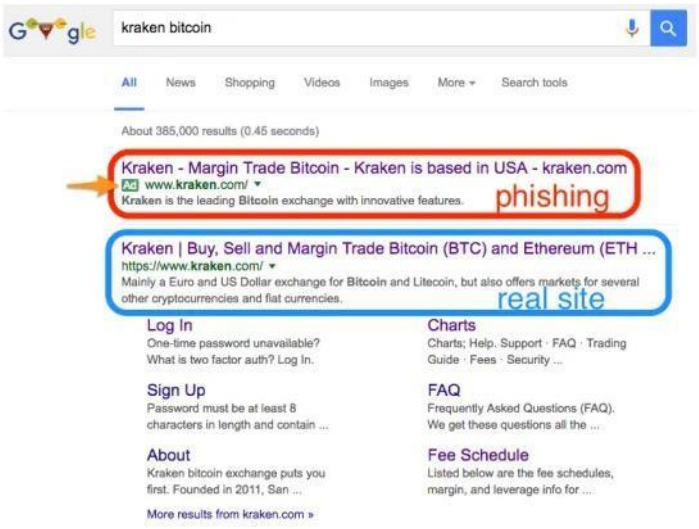
Esto puede ser evidenciado en la siguiente Figura:

[53] ANTONUCCI. Domenic. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. San Francisco: John Wiley & Sons, Incorporated. 2017. p.137. ISBN 9781119308805

[54] ACHILLES. What’s Search Engine Phishing and how to avoid it conveniently? [Sitio web]. [Consulta: 16 enero 2021]. Disponible en: https://www.achillesresolute.com/blog/what-is-search-engine-phishing.html

[55] DAY, Graham. Security in the Digital World: For the home user, parent, consumer and home office. Londres: IT Governance Ltd, 2017. p.64. ISBN 9781849289610

Figura 6. *Search engine phishing*.



Fuente: KRAKEN. Kraken *phishing* warning. [En línea]. San Francisco.: Security labs. 2016. (Recuperado en 16 mayo 2020) Disponible en: https://blog.kraken.com/post/225/kraken-*phishing*-warning/

5.1.10 *Phising* con evasión de filtros. Con las campañas en contra del *Phishing*, los delincuentes se idearon una manera para que los *software* o aplicaciones no detecten los documentos de ofimática adjuntos, eliminando los archivos relacionados con xml.rels con el que se identifica si contiene *malware*; este archivo mapea la relación de los archivos de office dentro y fuera, incluyendo en estos documentos el acceso a las paginas posiblemente falsas.

5.1.11 *Pharming* o *DNS-Based Phishing*. Es un tipo de ciberataque con el que se trata de redirigir el tráfico web a un sitio falso o malicioso, explotando vulnerabilidades conocidas de software en los sistemas de DNS, o en los terminales de los usuarios, esto permite a los atacantes redirigir un nombre de dominio a otra máquina distinta. De tal forma, que un usuario que introduzca un determinado nombre de dominio que haya sido redirigido, accederá en su explorador de internet a la página web que el atacante haya especificado. “Lo más habitual es que sea el usuario el que instale sin darse cuenta un software malicioso en su ordenador,

habitualmente recibido por correo electrónico u oculto junto a alguna descarga de *software*"[56].

5.1.12 *Malware-based phishing*. Este esquema se produce cuando el atacante adjunta un programa informático dañino hecho para simular ser útil en correos electrónicos, sitios *web* y otro tipo de documentos electrónicos en *Internet*. El *malware* envía la información al atacante que se encuentra conectado de manera remota. Un ejemplo de esto puede ser cuando el sitio *web* le solicita que instale un *plugin* o complemento para aumentar la seguridad de su equipo. Al hacer clic en el enlace y descargar el supuesto complemento, en realidad lo que acaba de descargar e instalar es *malware*. Este comúnmente implementa registradores de teclas (*keyloggers*) y registradores de pantalla (*Screenloggers*) para capturar las pulsaciones del teclado y los sitios que visita en Internet. El atacante está buscando algo (datos o información confidencial) y está dispuesto a ser tan paciente como sea necesario para adquirirlo[57]. De tal modo que estará atento al momento en el que la víctima haga clic.

5.1.13 *Content-Injection phishing*. "Es un escenario donde los piratas informáticos reemplazan parte del contenido de un sitio legítimo con contenido falso diseñado para engañar o desviar al usuario para que entregue su información confidencial al pirata informático"[58]. Por ejemplo, los atacantes pueden insertar código malicioso para registrar las credenciales del usuario o una superposición que puede recopilar información en secreto y entregarla al servidor de phishing del atacante.

5.1.14 *Watering Hole Phishing*, *watering hole attack*. Los ciber delincuentes no solo están adoptando mecanismos de phishing más avanzados, sino que también están

[56] GUERRERO, Diego, Fraude en la Red. Madrid. Ra-Ma Editorial. 2012. p.31. ISBN 9789587620665
[57] ALLSOPP, Wil. Advanced Penetration Testing: Hacking the World's Most Secure Networks. San Francisco: John Wiley & Sons, Incorporated. 2017. p.147. ISBN 9781119367680
[58] PC WORLD. Types of Phishing Attacks. [Sitio web]. California. Computer Associates. [Consulta: 20 de mayo 2020]. Disponible en: https://www.pcworld.com/article/135293/article.html

buscando nuevas formas de infiltrarse en el sistema de su objetivo. En un correo electrónico de phishing, un ciber delincuente intenta engañar al receptor para que proporcione su información confidencial o haga clic en un enlace malicioso. En una variación del phishing llamada ataque *Watering Hole Phishing*, en lugar de atacar objetivos, los ciberdelincuentes colocan una trampa para el usuario y esperan a que la presa los atrape.

5.1.15 *Evil Twin*. “Es un ataque en el que un atacante configura una red *Wi-Fi* falsa que parece un punto de acceso legítimo para robar los datos confidenciales de las víctimas. frecuentemente, las víctimas de tales ataques son personas o usuarios comunes”[59]. El ataque se puede realizar como un ataque de hombre en el medio (*MITM*). El falso punto de acceso *Wi-Fi* se utiliza para espiar a los usuarios y robar sus credenciales de inicio de sesión u otra información confidencial. Debido a que el atacante posee el equipo que se está utilizando, la víctima no tendrá idea de que podrían estar interceptando su información.

5.1.16 *Social Network Phishing*. Las redes sociales también son un método utilizado por los delincuentes para engañar a sus víctimas, ya que simplifica su trabajo. Con más de 1.300 millones de personas que inician sesión en sus cuentas de redes sociales cada mes, y la confianza que muchos tienen en la comunidad más amplia de usuarios, el *phishing* de redes sociales representa una rica fuente de ingresos para los estafadores.

5.1.17 *Phishing* 2.0. Consiste en hacer uso de un *proxy* inverso transparente para montar un ataque de tipo *man-in-the-middle* contra los usuarios. Este mecanismo intermediario hace que, en tiempo real sin que el usuario final se dé cuenta, todos los paquetes que provienen del navegador de la víctima, sea interceptado, y

[59] NORD VPN. How to identify and prevente vil twin attacks. [Sitio web]. Helsinki.: Green, Emily. [Consulta: 20 de mayo 2020]. Disponible en: https://nordvpn.com/es/blog/evil-twin-attack/

después es enviado al sitio *web*. De la misma manera en tiempo real cada paquete que proviene del sitio *web* será interceptado, antes de ser entregado al navegador.

Durante el proceso de interceptación, el proxy inverso analiza el contenido del paquete, realizando el almacenamiento de lo que considere útil (identificador de usuario, contraseñas o cookies de sesión) e incluso es posible modificar el contenido del paquete. Para poder usar estas técnicas con servidores web que usen https, es necesario que el servidor proxy tenga instalado un certificado https válido de una URL falsa que suplante a la URL del sitio web real.

Este tipo de ataque, al conseguir tener un control total del tráfico entre el navegador y el servidor, permite atacar sesiones con autenticación multifactor. Herramientas especializadas para automatizar este tipo de ataques son *Evilginx2* y *Modlishka*.

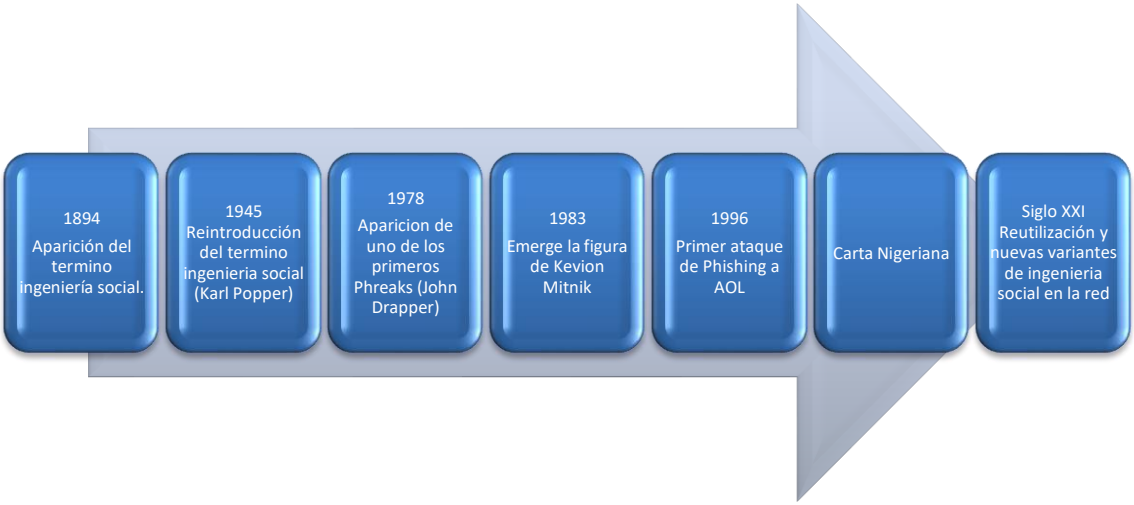
5.1.18 *Hishing* o "*hardware phishing*". Consiste en distribuir programa maligno ocultándolo en equipos que van a ser vendidos, ya sean estos nuevos o usados. Estos códigos maliciosos pueden ocultarse en teléfonos móviles, dispositivos y equipos.

5.2 EVOLUCION DE LA INGENIERIA SOCIAL

El uso de la expresión como tal de Ingeniería Social, surgió en 1894 gracias a un ensayo de *J.C. Van Marken* empresario y filántropo holandés, el cual tuvo difusión en Francia por *Émile Cheysson*, pero recibió un mayor impulso en Estados Unidos gracias al libro "*Social Engineering*" de W.H. Tolman, cuyo principal argumento es que no existe en las empresas una función social (departamento de recursos humanos en la actualidad), por lo que era requerido un ingeniero social con función de mediador para la resolución de los conflictos como intermediador racional entre el capital y el trabajo. En ese orden de ideas, un ingeniero social debía contar con

habilidades sociales, en contraste con el uso posterior del término. A continuación, se muestra una línea de tiempo en donde se resaltan los hechos más relevantes de la ingeniería social:

Figura 7. Línea de tiempo ingeniería social.



Fuente: elaboración propia

El concepto es generalizado y se tiene que la ingeniería social puede ser una técnica o método para lograr una variedad de resultados, es decir, deja de ser un instrumento para resolver problemas sociales y se transforma en uno para manipular a la población. Es evidente en este punto que la propaganda puede ser considerada ingeniería social, así como las campañas políticas y la religión, dado que buscan lograr un comportamiento específico en las masas. En 1945 *Karl Popper* reintroduce el término con la acepción de implementación de métodos críticos y racionales de la ingeniería y ciencia a los problemas sociales.

Con la llegada de *John Draper* más conocido como "*Captain Crunch*", esto porque gracias a un silbato que venía en las cajas de cereal el cual generaba un tono con frecuencia de 2600 *hertzios*, este tono era exactamente igual al tono de control de

los sistemas de telefonía de AT&T (en ese entonces *Bell*). Desarrollo una caja electrónica llamada *Blue Box* mediante la cual era posible tener acceso al sistema telefónico y realizar llamadas gratuitas.

Posteriormente aparece el legendario *Kevin Mitnik*, reconocido por sus múltiples hazañas en el campo del *hacking*, durante muchos años fue la peor pesadilla del Departamento de Defensa de Estados Unidos y de la NASA, ya que con gran facilidad podía acceder a sus sistemas. El propio *Mitnik* a través de sus libros ha reconocido que una de sus principales armas siempre fue la Ingeniería Social.

Por primera vez en enero de 1996 se hace mención del término *phishing* en el grupo de noticias de *hackers* alt.2600 y fue utilizado para describir a aquellos que intentaban "pescar" cuentas de correo de AOL. No obstante, es posible que este término ya hubiera aparecido anteriormente en la edición impresa del boletín de noticias hacker 2600 Magazine.

Los ataques de ingeniería social más comunes provienen de “phishing o spear phishing y pueden variar según los eventos actuales, los desastres o la temporada de impuestos. Debido a que la ingeniería social involucra un elemento humano, prevenir estos ataques puede ser complicado para las empresas”[60].

En el caso de *phishing* en AOL el atacante suplantaba a un empleado de AOL y hacia él envió de un mensaje a una víctima potencial. Para conseguir el engaño y que la víctima diera información confidencial, el mensaje de correo contenía textos como "verificando cuenta" o "confirmando información de factura". Una vez que el usuario enviaba sus credenciales de acceso, el atacante accedía a la cuenta de la víctima y la utilizaba para varios propósitos criminales, incluyendo el spam.

[60] HERNÁNDEZ DOMINGUEZ, Antonio, Sistema para la detección de ataques PHISHING utilizando correo electrónico. [Sitio web]. [Consulta: 10 de diciembre 2020]. Disponible en: https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/304

Figura 8. *Phishing* AOL Mail.

Fuente: LONDON´S EAST END GUARD DOG. Expired Mailbox *Phishing* Scam. [En línea]. Londres.: Londo´s east end. 2019. (Recuperado en 16 mayo 2020) Disponible en: https://mrbloggyguarddog.wordpress.com/2016/12/01/expired-mailbox-*phishing*-scam/

A finales de los años 90 se popularizó la famosa carta nigeriana, el Centro Cibernético Policial de Colombia, define esta estafa como: “Un engaño que consiste en ilusionar a la víctima con una fortuna inexistente y persuadirla para que pague una suma de dinero por adelantado, como condición para acceder a la supuesta fortuna”[61].

[61] CENTRO CIBERNETICO POLICIAL. Carta nigeriana herencia. [Sitio web]. Bogotá: Policía Nacional de Colombia. [Consulta: 10 de mayo 2020]. Disponible en: https://caivirtual.policia.gov.co/contenido/carta-nigeriana-herencia

5.3 ATAQUES DE INGENIERIA SOCIAL MÁS UTILIZADOS EN COLOMBIA

En el informe Tendencias del ciber crimen en Colombia, se estima que cerca de un 90% de los ciberataques a empresas en Colombia se deben a ingeniería social. La clave del asunto está en que el ciber delincuente necesariamente debe engañar a la víctima, para lograr este propósito gana su confianza o simula ser una persona o entidad que genera confianza, para lograr obtener acceso a la información.

Gracias a esto se han originado los BEC (*Bussines email compromise*), lo cual no es más que el compromiso a través de los correos electrónicos corporativos, cada vez es más frecuente encontrar que dentro de las organizaciones y grandes empresas, se habla de correos sospechosos o que su contenido no correspondía al contexto de la organización.

La Ingeniería Social y la explotación de vulnerabilidades siguen siendo los principales vectores que puede aprovechar un atacante para comprometer los servicios de una empresa. Los engaños basados en ingeniería social han evolucionado a lo largo de los años, volviéndose cada vez más efectivos.

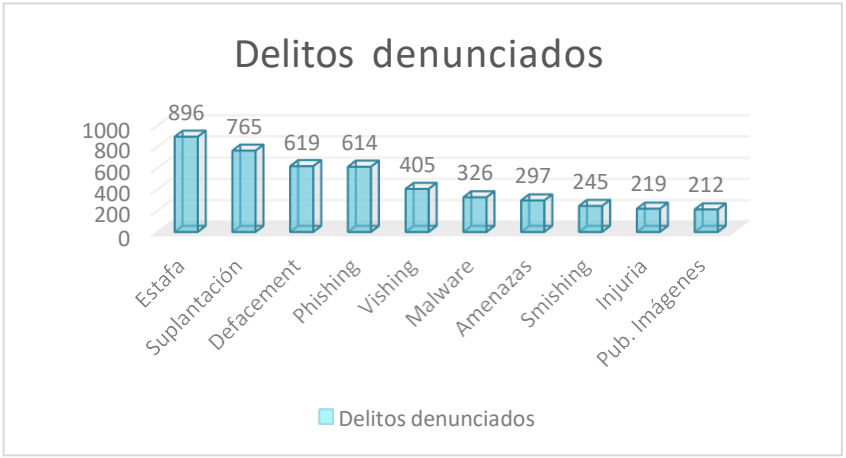
Para lograr determinar cuáles son los ataques de ingeniería social más utilizados en Colombia, se hace uso de la herramienta del CAI VIRTUAL de la Policía Nacional que permite, a través de un filtro temporal identificar la cantidad de delitos informáticos que se denuncian y bajo que modalidad fueron ejecutados los ataques. Para efectos de poder realizar el análisis con más detalle se realiza la búsqueda por años: 2016, 2017, 2018 y 2019. En la siguiente figura es posible evidenciar los resultados que se obtienen en el módulo de ciberincidentes.

Figura 9. Delitos reportados en 2016.

Fuente: CAI VIRTUAL. Ciber delitos, histórico. [En línea]. Bogotá.: Policía Nacional de Colombia. 2020. (Recuperado en 20 mayo 2020) Disponible en: https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

Para el año 2016, se logra evidenciar en Colombia que delitos relacionados a la ingeniería social como: estafa, suplantación, *phishing*, *vishing* y *smishing* ocupan los primeros lugares dentro de las denuncias realizadas. Como se logra evidenciar en la figura 10, el sector ciudadano ha sido el más afectado por este tipo de ataques.

Figura 10. Delitos informáticos denunciados en 2016.



Fuente: elaboración propia

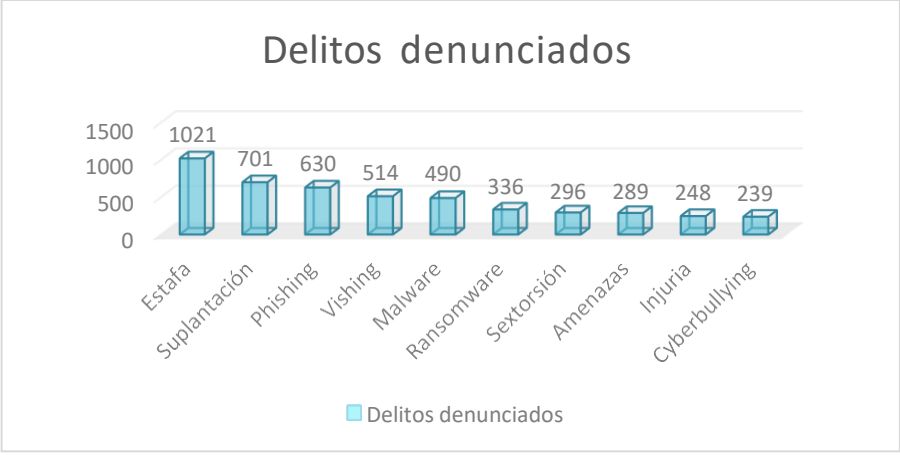
Es importante realizar el análisis de lo ocurrido en el año 2017, la figura 11 muestra los resultados obtenidos para este año.

Figura 11. Delitos reportados en 2017.

Fuente: CAI VIRTUAL. Ciber delitos, histórico. [En línea]. Bogotá.: Policía Nacional de Colombia. 2020. (Recuperado en 20 mayo 2020) Disponible en: https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

Para el año 2017, el comportamiento de los delitos asociados a la ingeniería social como: estafa, suplantación, *phishing* y *vishing* ocupan los cuatro primeros lugares dentro de las denuncias realizadas. Como se logra evidenciar en la figura 12, el sector ciudadano continúa siendo el más afectado por este tipo de ataques.

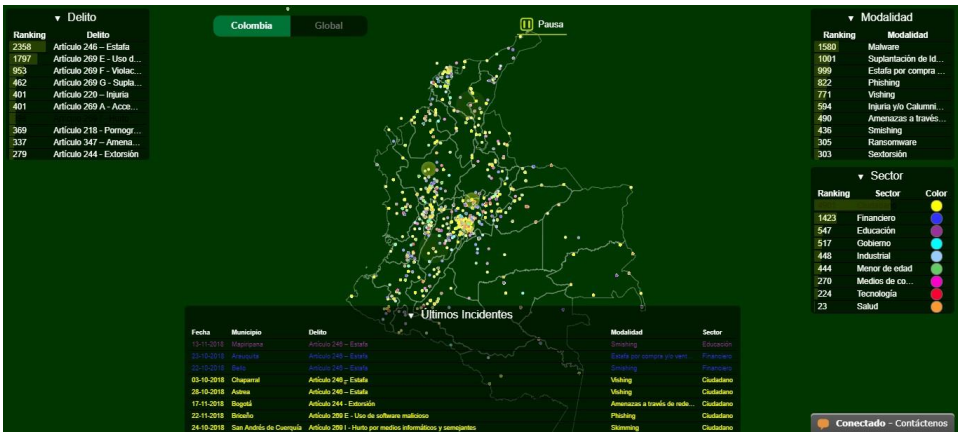
Figura 12. Delitos informáticos denunciados en 2017.



Fuente: elaboración propia

A continuación, se obtienen los datos arrojados por el CAI Virtual de la Policía Nacional, la figura 13 muestra los resultados obtenidos para el año 2018.

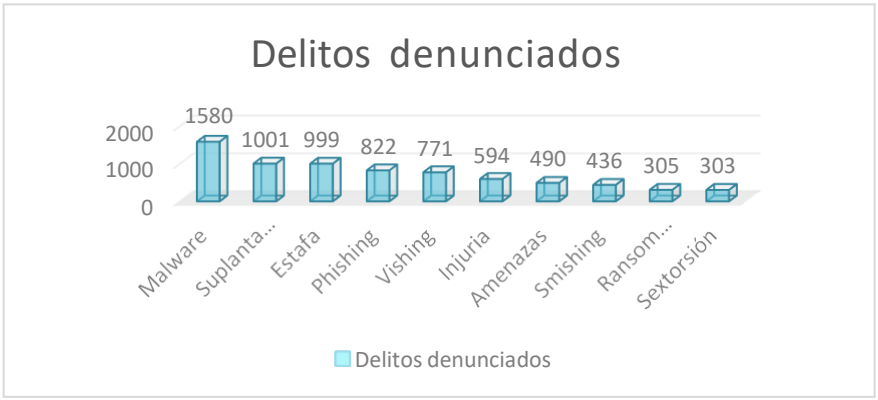
Figura 13. Delitos reportados en 2018.



Fuente: CAI VIRTUAL. Ciber delitos, histórico. [En línea]. Bogotá.: Policía Nacional de Colombia. 2020. (Recuperado en 20 mayo 2020) Disponible en: https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

En el año 2018, los delitos asociados a la ingeniería social continúan dentro del top 10 con modalidades como: suplantación, estafa, *phishing*, *vishing* y *smishing* se encuentran en los primeros lugares dentro de las denuncias realizadas. Como se logra evidenciar en la figura 14, el sector ciudadano continúa siendo el más afectado por este tipo de ataques.

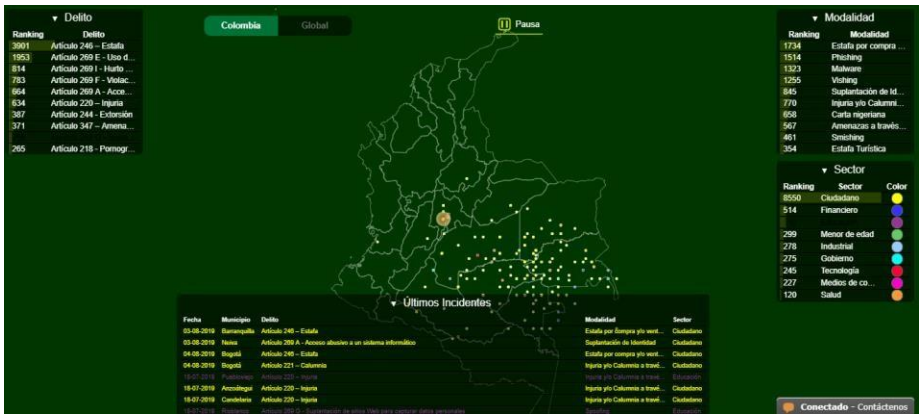
Figura 14. Delitos informáticos denunciados en 2018.



Fuente: elaboración propia

Finalmente se realiza la consulta en el aplicativo del CAI virtual sobre el comportamiento de los delitos informáticos denunciados, la figura 15 muestra los resultados obtenidos para el año 2019.

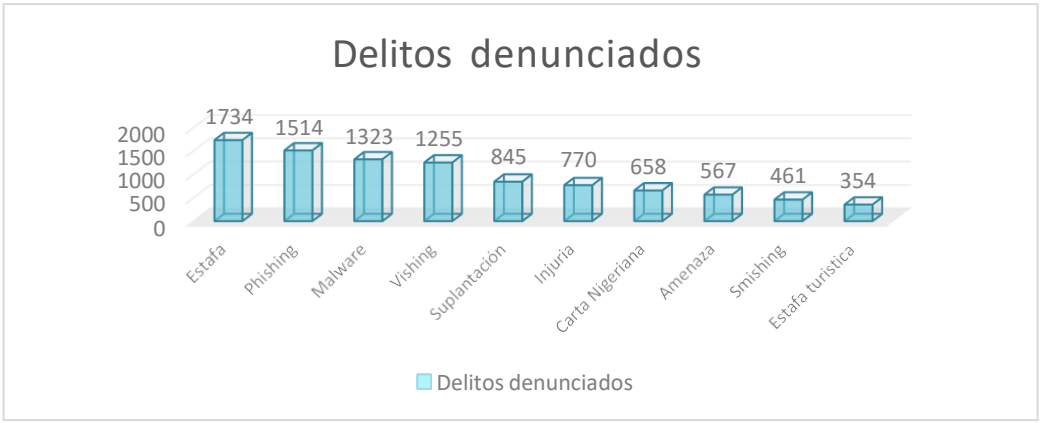
Figura 15. Delitos reportados en 2019.



Fuente: CAI VIRTUAL. Ciber delitos, histórico. [En línea]. Bogotá.: Policía Nacional de Colombia. 2020. (Recuperado en 20 mayo 2020) Disponible en: https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real/historico

En el año 2019 el comportamiento de los delitos asociados a la ingeniería social continúa dentro del top 10 con modalidades como: estafa, *phishing*, *vishing*, suplantación, carta nigeriana, *smishing* y estafa turística, tal y como se logra evidenciar en la figura 16.

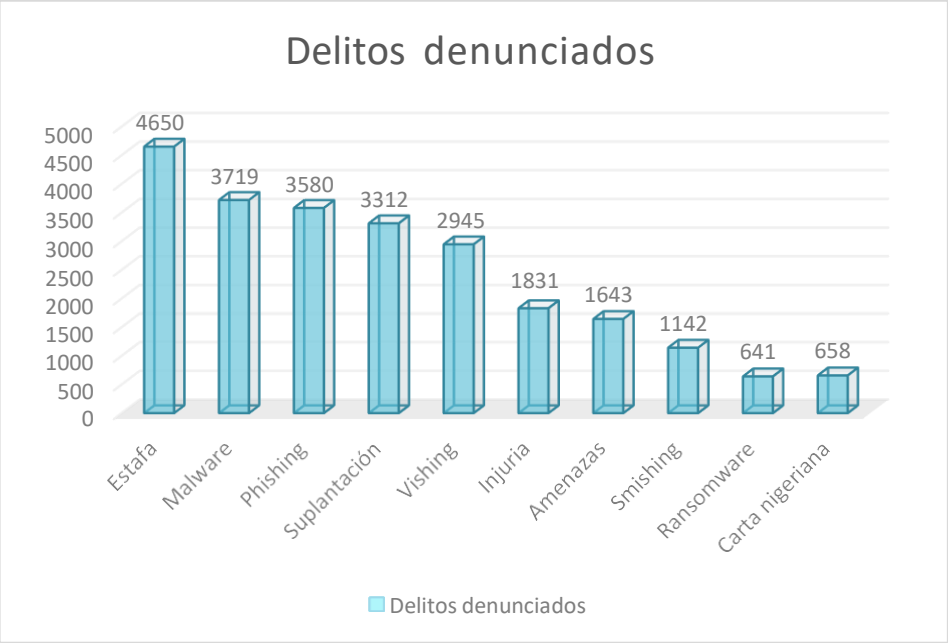
Figura 16. Delitos informáticos denunciados en 2019.



Fuente: elaboración propia

Para realizar una síntesis de lo encontrado gracias a la herramienta del CAI Virtual de la Policía Nacional de Colombia, se procede a compilar los datos para lograr obtener cuáles delitos asociados a la ingeniería social son los más comunes en Colombia, los cuales se muestran en la siguiente figura:

Figura 17. Delitos informáticos denunciados en 2016-2019.

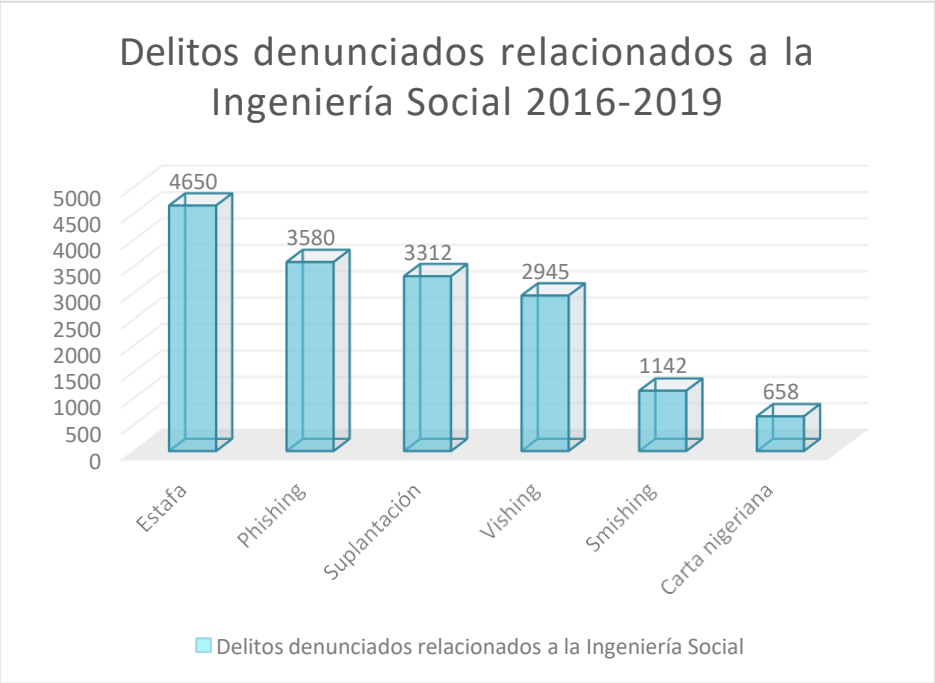


Fuente: elaboración propia

De acuerdo con el análisis de los datos anteriores, es posible deducir que, en el país una de las técnicas más utilizadas y que mayor impacto ha tenido, es la estafa con el 17 % en tercer lugar el *phishing* con el 13 % en cuarto lugar la suplantación con el 12% quinto lugar *Vishing* con el 10% octavo lugar para el *Smishing* con el 4% y finalmente la carta nigeriana en décimo lugar con el 2%.

Con el fin de resaltar y evidenciar de mejor manera lo anterior, es elaborada la gráfica que se muestra en la figura 18 que consolida los delitos más denunciados y que están relacionados a la ingeniería social, lo cual permite que sea posible dimensionar e identificar el comportamiento de este tipo de delitos en Colombia.

Figura 18. Delitos informáticos relacionados a la IS 2016-2019.



Fuente: elaboración propia

Con esto se obtiene que en el periodo seleccionado el 58% de los delitos informáticos denunciados en Colombia, están relacionados a técnicas de la ingeniería social. Un aspecto que llama la atención es la aparición en 2019 de la carta nigeriana, una de la técnica más antigua ha vuelto a aparecer en escena.

Tomando en cuenta los vectores de ataque es posible determinar que el 73 % de los ataques han sido mediante correos fraudulentos personalizados, lo que comúnmente se conoce como *phishing*. Aunque se tiene una categoría especial para esta técnica, las campañas de *malware* y *ransomware* se entregan haciendo uso del *phishing*. Por otra parte, según la Cámara Colombiana de Informática y Telecomunicaciones, los principales vectores de ataque en el 2019 son los que se muestran en la siguiente figura:

Figura 19. Principales vectores de ataque en 2019

Fuente: Cámara Colombiana de Informática y Telecomunicaciones. *Ransomware*, una ciberamenaza subestimada en Colombia [En línea]. Bogotá.: CCIT. 2019. (Recuperado en 20 mayo 2020). Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Jairo Hernán García Triana, coordinador de las especializaciones de Diseño y Seguridad en Redes Telemáticas de la Universidad El Bosque, asegura que: es necesario categorizar los crímenes contra las organizaciones y los que van contra la población en general. “En el primer caso, los más comunes en orden de peligrosidad son: el *ransomware*, el *phishing* y el *malware*, mientras que en la seguridad personal están el ciberacoso, el *sexting* y el robo de identidad”[62].

[62] Portafolio. Conozca las formas de fraude en la web: Los delitos informáticos más comunes en las compañías son ‘phishing’, ‘ransomware’ y ‘malware’. [en línea]. [Consulta: 22 de octubre de 2020]. Disponible en: https://bv.unir.net:2257/docview/2295404820/fulltext/582DFCC6177741A0PQ/1?accountid=142712

5.4 ESTRATEGIAS PROPUESTAS POR PARTE DE LAS ENTIDADES DEL ESTADO COLOMBIANO PARA LA MITIGACIÓN DE LOS ATAQUES DE INGENIERÍA SOCIAL.

En cuanto a la generación de estrategias que contribuyan a mitigar el riesgo asociado a los ataques de ingeniería social, el estado colombiano y entidades del sector privado han diseñado estrategias para que los ciudadanos aprendan a identificar ataques de este tipo y si en determinado momento han sido víctimas ha creado los canales por los cuales puede realizar la respectiva denuncia y poner en conocimiento de las autoridades la ocurrencia del hecho.

- **colCERT - Grupo de Respuesta a Emergencias Cibernéticas de Colombia.**

http://www.colcert.gov.co/

Este grupo tiene como finalidad y principal responsabilidad la coordinación de la Ciberseguridad y la Ciberdefensa Nacional, que estará en el marco del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. El propósito principal es la coordinación de acciones necesarias para proteger la infraestructura crítica del Estado colombiano frente a cualquier emergencia relacionada con la ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

Dentro de sus objetivos se mencionan los que tienen relación directa con el tema de estudio:

- Coordinar y asesorar a CSIRT's y entidades tanto del nivel público, como privado y de la sociedad cívil para responder ante incidentes informáticos.
- Ofrecer servicios de prevención ante amenazas informáticas, respuesta frente a incidentes informáticos, así como a aquellos de información, sensibilización y formación en materia de seguridad informática.

De igual forma se realizan publicaciones sobre alertas e información que le permiten a la ciudadanía en general conocer nuevas amenazas que se encuentran disponibles en la red.

- **CSIRT-PONAL - Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía Nacional.** https://cc-csirt.policia.gov.co

Este grupo fue creado con el propósito de atender las necesidades en cuanto a la prevención, atención e investigación de eventos e incidentes de seguridad informática, esto con el fin de proteger la infraestructura tecnológica, activos de información y mitigar el impacto ocasionado por la materialización de los riesgos asociados con el uso de las tecnologías de la información y las telecomunicaciones.

Uno de los objetivos del CSIRT es proveer asistencia técnica, asesoría y apoyo a la comunidad y a las organizaciones públicas o privadas, en cuanto a la protección ante amenazas y/o incidentes informáticos. De la misma manera consolidar procesos y procedimientos de atención de incidentes de seguridad de la información mediante el uso de estándares y buenas prácticas. También activar mecanismos de colaboración para la coordinación y gestión de incidentes entre entidades.

- **CSIRT Financiero – Equipo de apoyo para la respuesta a incidentes de Ciberseguridad para el sector financiero colombiano.** https://csirtasobancaria.com

Este equipo ha sido desarrollado por la Asociación Bancaria y de Entidades Financieras de Colombia, Asobancaria. Con el fin de proporcionar apoyo y respuesta ante incidentes que afectan al sector financiero y a la vez fomenta la colaboración entre sus miembros e intercambio de información para afrontar de mejor manera las amenazas cibernéticas. El equipo, es altamente calificado y

contribuye en procesos de gestión de riesgos y seguridad de datos con el fin de crear espacios digitales seguros.

Las funciones específicas de este equipo de respuesta son:

- Proporcionar apoyo a entidades financieras para el fortalecimiento de capacidades preventivas y reactivas.
- Fortalecer estándares de ciberseguridad que se han implementado en el sector financiero en Colombia.
- Constituirse como eje central del sector financiero en cuanto a la gestión de crisis e incidentes de seguridad informática.
- Tomar la vocería frente a las autoridades nacionales en materia de ciberseguridad.
- Ser los principales promotores de la comunidad de intercambio de información de ciberseguridad del sector financiero con organismos nacionales e internacionales.

- **Sistema Nacional de Denuncia Virtual ... ¡ADenunciar!** https://adenunciar.policia.gov.co/Adenunciar/Login.aspx

Este sistema que se ha implementado en conjunto entre la Policía Nacional y la Fiscalía General de la Nación permite que los ciudadanos puedan dar trámite a las diferentes solicitudes que están habilitadas en este sistema, pero para esto se requiere del registro del ciudadano.

A denunciar! le permite al ciudadano realizar 6 tipos de denuncias virtuales las cuales serán atendidas por funcionarios de la policía judicial, siendo estos los encargados de validar si la información califica como denuncia penal, posteriormente realizara el trámite correspondiente que haya lugar.

Los delitos que se pueden denunciar son los siguientes:

- Hurto a Comercio

- Hurto a personas
- Hurto a residencias
- Delitos Informáticos
- Pornografía Infantil
- Extorsión

En el caso de estudio, dentro de los delitos informáticos que se pueden denunciar son aquellas conductas en que el o los delincuentes se valen de programas informáticos para cometer delitos como implantación de virus, suplantación de sitios web, estafas, violación de derechos de autor, piratería, etc.

- **CAI Virtual** https://caivirtual.policia.gov.co/

En el cai virtual de la Policía Nacional de Colombia, los ciudadanos pueden encontrar el medio que les permite reportar incidentes informáticos, también cuenta con un mural del cibercrimen en donde se exhiben muestras de las diferentes modalidades que utilizan los ciberdelincuentes para tratar de afectar a las personas, por otra parte se encuentra la publicación de boletines en donde se muestran las nuevas amenazas y la manera en la que se ejecutan los ataques informáticos, allí se pueden encontrar las recomendaciones, guías e informes que contribuyen a generar en los ciudadanos una cultura de auto cuidado en aspectos de los sistemas informáticos y el uso de TICS.

Cuenta con un mapa que muestra un reporte del comportamiento del delito informático en Colombia, esto permite que se evidencie la ocurrencia de este tipo de hechos y los ciudadanos entiendan que ataques relacionados a la ingeniería social suceden todos los días y en nuestro país son más comunes de lo que se piensa.

5.5 BUENAS PRÁCTICAS Y RECOMENDACIONES PARA QUE LAS PERSONAS NO SE VEAN AFECTADAS POR ATAQUES DE INGENIERÍA SOCIAL.

De acuerdo con el análisis realizado, en Colombia se mantiene la tendencia en el periodo de 2016 a 2019 por parte de los ciberdelincuentes el uso de técnicas relacionadas a la Ingeniería Social, de tal forma que se identifican 6 modalidades que representan un riesgo para los usuarios de internet en nuestro país. Por lo tanto, se proponen unas buenas prácticas y recomendaciones para que las personas no se vean afectadas por ataques de este tipo.

5.5.1 Estafa. Aunque directamente la estafa no es una técnica de Ingeniería Social, si utiliza muchos de sus elementos, ya que normalmente se engaña a la persona para proceder con la estafa. Los delincuentes utilizan planes muy creativos para lograr engañar a muchas personas cada año. La tendencia actual es incorporar a las nuevas tecnologías los viejos trucos con el fin de lograr que las personas les envíen dinero o proporcionen información personal. A continuación, se ofrecen algunos consejos prácticos que le ayudarán a mantenerse en cierta medida más seguros.

- Detectar a los impostores. Los estafadores normalmente se hacen pasar por alguien en quien la victima confía, como lo puede ser: un funcionario de una entidad del gobierno, algún miembro de la familia, una organización benéfica, una entidad financiera o una empresa con la que hace o ha hecho negocios. Por ningún motivo entregue información personal respondiendo ese tipo de solicitudes inesperadas, ya sea como un mensaje de texto, una llamada telefónica o un correo electrónico, y por ningún motivo envíe dinero.

- Verifique la información, a través de una búsqueda en línea. Al digitar el nombre de determinada empresa o producto en el buscador de su preferencia

incluya palabras como "revisión", "queja" o "estafa", esto traerá resultados que le pueden ayudar a aclarar la situación, o realice una búsqueda que describa la situación, como "Llamada de Banco". Si lo prefiere, también puede buscar los números de teléfono de los cuales se han comunicado para ver si están relacionados a alguna estafa o si otras personas los han denunciado.

- No se debe confiar totalmente en el identificador de llamadas. Actualmente la tecnología permite que sea posible falsificar la información del identificador de llamadas, es por esto por lo que el nombre y el número que se visualiza en pantalla no siempre es real. Si por algún motivo alguien llama solicitando dinero o datos personales, simplemente cuelgue. Si tiene dudas o cree que la persona que ha llamado podría estar diciendo la verdad, vuelva a llamar a un número que sepa que es legítimo o comuníquese con la entidad que dice representar.

- No se debe pagar por adelantado. Un estafador podría pedirle que realice un pago adelantado por cosas como: alivio de deudas, ofertas de crédito y/o préstamos, asistencia hipotecaria o una oferta de trabajo. Incluso, uno de los más usados es manifestar que ganó un premio, pero antes debe pagar algún impuesto o tarifa para que se haga efectiva la transacción. Si decide realizar el pago, probablemente cobrarán el dinero y desaparecerán.

- Las tarjetas de crédito cuentan con protección antifraude, pero algunos métodos de pago no incorporan esta medida de protección. Cuando se realizan transferencias de dinero mediante servicios como Western Union o MoneyGram es más arriesgado, esto porque es casi imposible recuperar el dinero. Eso también sucede con las tarjetas recargables o de regalo. Las entidades del gobierno y las empresas honestas nunca exigirán que utilice estos métodos de pago.

- Antes de entregar su dinero o información personal, hable con alguien de su confianza, tómese el tiempo para analizar lo que está sucediendo. Los estafadores

normalmente presionan a las personas para que tomen decisiones rápidamente. Incluso pueden llegar hasta a amenazarle. A partir de esto tome las cosas con calma, analice la situación, realice una búsqueda en internet sobre el caso o situación, consulte a un experto o simplemente cuéntele a un familiar o amigo.

5.5.2 ***Phishing.*** Es fundamental tener claro que el antivirus es solo una pequeña parte en cuanto a la protección contra phishing. La intervención del usuario final influye de manera significativa al momento de evitar este tipo de ataques.

Figura 20. Ejemplo de phishing

Fuente: elaboración propia

Como se puede evidenciar en la figura 20 hay varios signos de alarma que indican claramente que el mensaje no es legítimo. Inicialmente al verificar el remitente se observa que el correo proviene de “so van hoa the thao va du lich” lo cual de entrada genera desconfianza ya que es un nombre inusual, por otra parte, el correo del que proviene “sovhttdl@phutho.gov.vn” no está relacionado con ningún dominio de Microsoft, en la parte inferior se hace referencia al “Equipo de verificación de Microsoft” pero el correo del remitente está en un dominio @phutho.gov.vn que no tiene relación alguna.

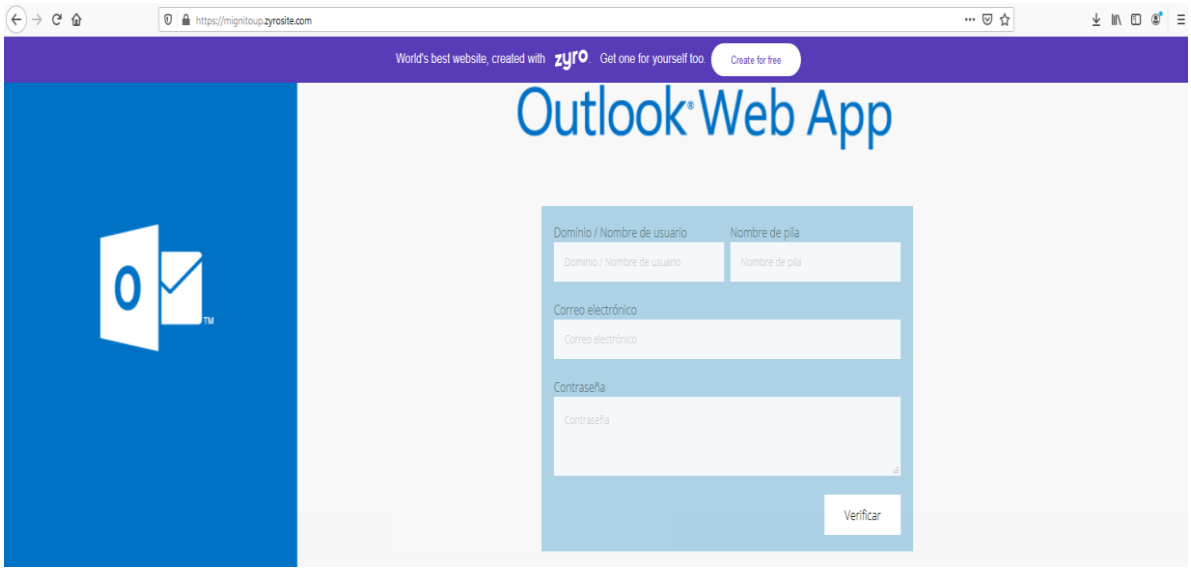
Para aparentar legitimidad en el mensaje aparentemente se envía esta misma información a una cuenta de Outlook para notificar sobre la situación del buzón afectado, un aspecto fundamental es el carácter de urgencia del mensaje, puesto que como se puede evidenciar en la figura 20 se hace creer al usuario que esta notificación ya se ha enviado en múltiples ocasiones y que esta es la última oportunidad de subsanar la novedad, de lo contrario la cuenta de correo será bloqueada. Para que esto no suceda deberá actualizar sus credenciales de acceso, con esto el atacante busca que el usuario proporcione la clave actual de la cuenta de correo.

Finalmente aparece otro actor importante en este tipo de ataques, los enlaces maliciosos, puesto que su objetivo es llevar al usuario a un sitio web fraudulento en el que solicitará el supuesto cambio de clave y para hacerlo deberá proporcionar la clave actual, aunque no solamente pueden obtener la clave ya que el sitio al que dirigen al usuario puede contener código malicioso que se ejecute al momento de ingresar e infectar la máquina. Al pasar el cursor sobre el enlace se puede visualizar en la parte inferior izquierda que apunta a “https://mignitoup.zyrosite.com” que tampoco tiene ningún tipo de relación con *Microsoft*.

Al ingresar a esa URL el usuario se encuentra con un supuesto formulario de *Outlook* que le permitirá validar su identidad, pero a través de este sitio lo único que buscan es conseguir la cuenta de correo y la contraseña.

En la figura 21 se observa un formulario elaborado por el atacante, el cual trata de engañar a la víctima utilizando el logo y nombre de la aplicación de correo electrónico de *Outlook.*

Figura 21. Formulario creado por el atacante



Fuente: elaboración propia

Como es posible evidenciar en la *URL* aparece el https pero no está resaltado en verde lo que demuestra que no se ha validado la autenticidad del certificado. Aunque el usuario no debería haber llegado a este punto, puesto que como se menciona anteriormente el sitio puede estar infectado, pero si ya ha hecho clic en el enlace se visualiza la publicidad del servicio de alojamiento gratuito (*zyro*) que han utilizado y una compañía tan grande como *Microsoft* no utilizaría este tipo de servicios y más aún para validar cuentas de correo.

Adicionalmente a lo manifestado en el ejemplo de phishing, se sugiere a los usuarios lo siguiente con mayor detalle:

- Tener precaución al hacer clic en hipervínculos o enlaces que vienen dentro de correos electrónicos, *SMS* (mensajes de texto) o mensajes instantáneos, incluso si parecen haber sido enviados desde una fuente conocida o confiable. Para asegurarse a donde lo redirigirá, ubique el cursor sobre el enlace antes de hacer clic en ellos en la parte inferior izquierda de la ventana aparecerá la dirección a la

cual será redireccionado, esto para verificar que la *URL* lo lleve a un sitio web legítimo, adicionalmente, jamás en ninguna circunstancia proporcione su contraseña, número PIN o cualquier otro dato confidencial. Si el mensaje le genera alguna duda, lo mejor es consultar directamente con el remitente antes de hacer clic en algo que se considera como sospechoso.

- Mantener el navegador actualizado. Esta práctica realmente es muy sencilla de incorporar a los hábitos digitales ya que únicamente se debe garantizar y permitir que los navegadores se actualicen cada vez que el fabricante publica una nueva versión. Las empresas desarrolladoras publican con regularidad actualizaciones o parches para corregir las vulnerabilidades de seguridad que se han encontrado en su *software*. Actualizar siempre el navegador, el sistema operativo y demás aplicaciones cuando sea solicitado, esto es fundamental para robustecer la seguridad de todo el sistema, y como medida adicional habilitar las actualizaciones automáticas, esto siempre y cuando sea posible.

- Verificar que la página web sea segura. Este aspecto siempre debe ser tenido en cuenta, sobre todo antes realizar el ingreso de información confidencial (esto incluye nombres de usuario y contraseñas), se debe asegurar de verificar que el sitio sea seguro. La forma más sencilla de hacer esta verificación es confirmar que la URL de la página web comienza con HTTPS y que hay un icono de candado en la barra de direcciones. En algunos casos los sitios web también muestran sellos de confianza, esto para indicar que el sitio es seguro. Si el navegador o el antivirus identifica a un sitio *web* de *phishing*, este lo alertará de manera inmediata y procederá a bloquear el acceso al sitio. No debe ignorar estas advertencias, solo si se está cien por ciento seguro de que se trata de un falso positivo.

- Una buena práctica es instalar una extensión en el navegador *anti-phishing*. Algunos navegadores traen incorporada una protección contra phishing bastante robusta, pero puede llevar la seguridad a un nivel más alto realizando la instalación

de una extensión de navegador *anti-phishing* dedicada. Recientemente, Microsoft lanzó *Windows Defender Browser Protection*, actualmente únicamente es compatible con *Google Chrome*.

- Conocer el lenguaje que se utiliza en una suplantación de identidad. Los ataques de suplantación de identidad se caracterizan por parecer muy convincentes. Para identificar un correo electrónico o un mensaje instantáneo sospechoso lo mejor es familiarizarse con el lenguaje que se utiliza en ataques de phishing. Esto puede incluir:

- Errores gramaticales, tipográficos y frases que no encajan, puesto que suenan poco profesionales o fuera de contexto.
- Palabras o situaciones que crean un sentido de urgencia.
- Se solicita verificar la cuenta ya sea bancaria o de correo, teléfono, dirección, datos bancarios y cualquier otra información confidencial.
- Saludos en los que se dirigen a usted como "Cliente" cuando se supone que la entidad tiene los datos debería usar el nombre y / o apellido real.

- Es recomendable digitar las URL y utilizar marcadores para evitar hacer clic en enlaces, puesto que cuando esto se hace en enlaces que vienen en correos electrónicos puede existir un alto riesgo para los usuarios. En su lugar, basta con abrir el navegador y escribir de forma manual la URL de la entidad o empresa de la que ha recibió el correo electrónico. Por otra parte, marcar los sitios web que utiliza con frecuencia y abrirlos rápidamente desde el navegador cuando sea necesario; pero antes debe asegurarse que los sitios efectivamente son legítimos y si los son puede marcarlos.

- El *phishing* no afecta únicamente a la banca en línea. Normalmente se tiende a asociarlo con este tipo de banca, pero es importante mencionar que los ataques del tipo phishing se utilizan también para suplantar o hacerse pasar por una

organización o individuo, y los efectos pueden ser igual de devastadores que un fraude bancario, puesto que el atacante apunta a obtener beneficio económico. Por ejemplo, al perder las credenciales de acceso del correo electrónico o de las cuentas en redes sociales puede traer consecuencias graves y con alcance en la vida personal y profesional. Cuando se produce el robo de las credenciales de inicio de sesión de un sitio o servicio, también puede afectar otras cuentas si se usan las mismas contraseñas para otros servicios en línea.

- Este muy atento a las ventanas emergentes. Afortunadamente, esto se ha venido controlando desde los navegadores, pero aún se utilizan en algunos sitios *web*. Sea muy cuidadoso cuando ingrese datos o información en este tipo de ventanas, puesto que ha habido casos de ataques relacionados con el *phishing* en este tipo de ventanas que se hacen pasar como una parte legítima del sitio *web* principal. *Firefox*, *Google Chrome* y *Microsoft Edge* cuentan con configuraciones integradas que contribuyen a bloquear las ventanas emergentes.

- No solamente es el correo electrónico. Hay que tener presente que existen otros vectores de ataque, la forma más utilizada para el envío de ataques de *phishing* es el correo electrónico, pero eso no quiere decir que otros canales de comunicación sean más seguros. Existen ataques en las redes sociales, los cuales se han popularizado en los últimos años, y los investigadores en seguridad informática incluso han detectado aplicaciones de *phishing* maliciosas publicadas en *Google Play*. De tal forma que se resalta la importancia de estar muy atento al momento de transmitir datos en cualquier dispositivo que se conecte a Internet, sin importar la aplicación que esté utilizando o el medio de comunicación.

En el ámbito empresarial se pueden implementar ciertas medidas para protegerse contra el *phishing*:

- Educar a los empleados es fundamental y realizar sesiones de capacitación con escenarios de *phishing* simulados.
- Implementar un filtro de *SPAM* que detecte virus, remitentes en blanco, etc.
- Mantener todos los sistemas actualizados con los últimos parches y actualizaciones de seguridad.
- Instalar una solución antivirus, programar actualizaciones de firmas y controle el estado del antivirus en todos los equipos.
- Desarrollar una política de seguridad que incluya, pero no se limite a la caducidad y complejidad de la contraseña.
- Implementar un filtro *web* para bloquear sitios web maliciosos.
- Cifrar toda la información confidencial de la empresa.
- Convertir el correo electrónico HTML en mensajes de correo electrónico de solo texto o desactive los mensajes de correo electrónico HTML.
- Implementar cifrado para los empleados que trabajan a distancia.

5.5.3 Suplantación. La suplantación de identidad en línea no es lo mismo que tener la cuenta de redes sociales comprometida; se hace referencia a que una persona malintencionada configure una cuenta completamente diferente, pero muy similar a su nombre y con su foto de perfil existente. Cuando esto sucede alguien está tratando de engañar a sus contactos en las redes sociales para que hagan algo que beneficie al atacante (comúnmente, transferir dinero), o que la persona quiere dañar la reputación de la víctima.

- Revise su lista de amigos / contactos. Esta actividad es muy importante porque al asegurarse de estar conectado a través de las redes sociales solo con personas que realmente conoce o con las que tiene una relación de amistad o en las que al menos se puede confiar, puede contribuir a detectar perfiles sospechosos. Los estafadores a menudo envían solicitudes de amistad a las personas para

obtener detalles sobre sus vidas, que luego pueden utilizar maliciosamente en su contra.

- En el caso de encontrar cuentas que estén suplantando su identidad o de alguien que conoce se debe denunciar la cuenta, en el caso de ser una suplantación de su perfil, inmediatamente publicar en las redes sociales comprometidas varias advertencias con el fin de alertar a los contactos sobre alguien está suplantando la identidad y que se proceda a bloquear esa cuenta de inmediato.

- No contactar al suplantador. Esto es una pérdida de tiempo, puesto que ponerse en contacto con el impostor y acusarlo o pedirle que detenga su actividad genera que este trate de engañar a los contactos de manera más rápida. Al contactar al estafador puede suceder que trate de engañar o solicitar dinero para dejar de suplantar o que incremente las actividades fraudulentas en el perfil falso con el fin de obtener beneficio antes de que le bloqueen la cuenta.

5.5.4 *Vishing.* El phishing de voz, mejor conocido como *vishing*, se produce cuando un delincuente intenta obtener información a través de una llamada telefónica. De hecho, las estafas más elaboradas utilizan una combinación de fraude por correo electrónico y voz para parecer más legítimas y engañar de forma más sencilla a la víctima. A partir de lo anteriormente mencionado es fundamental identificar este tipo de llamadas y tener en cuenta algunas recomendaciones para evitar ser víctima de este ataque.

- Bloquear las llamadas automáticas. Este tipo de llamadas se realizan de manera automatizada normalmente mediante un mensaje grabado. Los estafadores también utilizan marcadores automáticos para realizar una gran cantidad de llamadas en cuestión de pocos minutos, por lo que tienen más posibilidades de comunicarse con una persona real.

Puede bloquear de forma manual los números maliciosos desde su teléfono inteligente para realizar este procedimiento debe consultar el manual del teléfono o consulte a su operador de telefonía para obtener instrucciones específicas.

- No responda números desconocidos. Bloquear números de teléfono no detendrá los intentos de *vishing* porque los estafadores usan software para codificar su número de teléfono real. Por ejemplo, los estafadores suelen imitar el código de área y los primeros tres dígitos de su número de teléfono para engañar a las víctimas y hacerles creer que es una llamada local. Si bloquea un número, los estafadores simplemente lo llamarán desde otro.

Si la victima contesta el teléfono y luego cuelga inmediatamente, el estafador sabrá que la línea está activa. Sin embargo, si no levanta el teléfono, los estafadores eventualmente considerarán que su número está inactivo. Es recomendable no responder llamadas desconocidas, y debería ver que la frecuencia con la que recibe las llamadas automáticas comienza a disminuir.

- Si recibe una llamada informándole de actividad inusual en una de sus cuentas, trate de sospechar de la información que está recibiendo. La persona al otro lado de la línea puede incluso tener parte de su información personal, pero eso no significa que sea una autoridad real. No confirme ni niegue la información que le proporcionen, y no proporcione ninguna información propia. Lo mejor que se puede hacer en estos casos es colgar el teléfono y llamar directamente a la organización que afirman representar. No confíe en la información de contacto proporcionada por la persona que lo llamó. Si es un estafador, esta información simplemente lo enviará a través de canales no oficiales.

5.5.5 *Smishing.* La tecnología ha facilitado muchos aspectos de la vida cotidiana, son muchos los beneficios, pero también ha abierto otras formas de ser estafados.

En el caso de recibir un mensaje de texto de un número desconocido que promete librar de las deudas hipotecarias hay que empezar a desconfiar.

A continuación, se enumeran algunas prácticas útiles para evitar estos ataques, en primera instancia debe buscar los mismos signos que buscaría en un correo electrónico que fuera un intento de *phishing,* luego debe:

- Verificar si hay errores ortográficos y gramaticales.
- Visitar el sitio web del remitente en lugar de proporcionar información en el mensaje.
- Verificar la información del remitente. dirección de teléfono para asegurarse de que coincida con la de la empresa a la que pretende representar.
- No proporcionar información financiera o de pagos sobre nada que no sea el sitio web de confianza.
- No hacer clic en enlaces de remitentes desconocidos o en aquellos que le generen desconfianza.
- Tener cuidado con "responder rápido", "registrarse ahora" u otras ofertas agresivas y demasiado buenas para ser verdad.
- Escribir siempre direcciones web en un navegador en lugar de hacer clic en el enlace.
- Instalar un antivirus compatible con dispositivos móviles en sus dispositivos inteligentes.

5.5.6 Carta nigeriana. Este tipo de estafa es muy antiguo y en los tiempos modernos los estafadores utilizan la tecnología para tratar de engañar a más personas, por esta razón hacen uso de correo electrónico. Esto funciona de manera similar al *phishing* y combina elementos de la estafa y la suplantación, por lo tanto, las mismas recomendaciones expresadas anteriormente son efectivas con este tipo de ataque.

6. CONCLUSIONES

- Los ataques de ingeniería social han evolucionado de tal forma que cada vez es mucho más complicado para los usuarios identificar este tipo de amenazas, desde los inicios de internet se han conocido casos de ataques de este tipo, y a pesar de esto aún los delincuentes hacen uso de las mismas técnicas, pero incorporando nuevas tecnologías para engañar a las personas.

- El ciber crimen en Colombia, ha tenido un crecimiento exponencial durante los últimos años de forma paralela al uso de las nuevas tecnologías y acceso a dispositivos móviles. Las pérdidas económicas generadas por los ciberataques asociados a la ingeniería social sitúan a esta problemática como una de las principales actividades ilegales en el País.

- Para los atacantes la ingeniería social se ha convertido en su primera opción al momento de ejecutar un ataque, puesto que gracias a los diferentes métodos y técnicas se logra obtener mayor efectividad. Como se logra identificar es una problemática real y es prioritario tomar medidas al respecto.

- La cantidad de delitos informáticos que son denunciados en Colombia como fue posible evidenciar son bastantes, pero el escenario que más preocupa es el aumento desde el año 2016 y que no todas las victimas denuncian la ocurrencia de este tipo de eventos.

- Al aprovechar las debilidades humanas naturales, las estafas del tipo *phishing* continúan siendo un tipo de ataque común y eficaz, ya que su porcentaje de éxito radica en que el atacante envía miles de correos y al afectar un pequeño grupo de estos puede obtener el beneficio económico. Es importante contar con un software antivirus, toda vez que cumplen un rol importante que desempeñar en la prevención de ataques de phishing, pero el usuario debe asegurarse que su

antivirus realmente combate el phishing y los riesgos de seguridad y privacidad que esto implica.

- Toda organización cuenta con el factor humano, por lo tanto, los humanos, por naturaleza, es curioso, propenso a tomar decisiones de manera rápida y, con frecuencia, están guiados por las emociones. Por esta razón, es fundamental que desarrolle un conjunto de herramientas de ingeniería social para contribuir a reforzar la seguridad contra los ataques de este tipo que normalmente aprovechan las vulnerabilidades humanas.

7. RECOMENDACIONES

Los ingenieros sociales son especialistas en manipular los sentimientos humanos, como la curiosidad o el miedo, esto para atraer a las víctimas y que caigan en las trampas. Por lo tanto, se debe tener mucho cuidado siempre que un correo electrónico genere algún sentido de alarma o urgencia, estar alerta puede contribuir a proteger a los usuarios contra la mayoría de los ataques de ingeniería social que se ejecutan en el ámbito digital. Además, los siguientes consejos pueden ayudar a mantener bajo control los ataques de ingeniería social.

No abrir correos electrónicos y archivos adjuntos de fuentes sospechosas: si no se conoce al remitente, no es necesario responder el correo electrónico. Incluso si se conoce y se sospecha del mensaje, se debe verificar y confirmar directamente, puede ser por teléfono o directamente desde el sitio web de la entidad suplantada.

Las direcciones de correo electrónico se falsifican todo el tiempo; incluso un correo electrónico que supuestamente proviene de una fuente confiable puede haber sido falsificado por un atacante, por esta razón se debe sospechar de los mensajes que realizan solicitudes inusuales o directamente piden datos personales.

Utilizar la autenticación multifactor: los delincuentes tratan de obtener las credenciales de acceso, el uso de un segundo factor de autenticación ayuda a garantizar la protección de las cuentas en caso de que el sistema se vea comprometido.

BIBLIOGRAFÍA

ACENS TECHNOLOGIES. Qué es el phishing y cómo protegerse. [Sitio web]. Madrid: Telefónica. [Consulta: 15 de abril 2020]. Disponible en: https://www.acens.com/wp-content/images/2014/10/wp-phising-acens.pdf

AENOR. Seguridad en Sistemas de Información Un recorrido a vista de pájaro. [Sitio web]. Ciudad Real. [Consulta: 1 de mayo 2020]. Disponible en: https://ruidera.uclm.es/xmlui/bitstream/handle/10578/2302/Seguridad%20en%20Sistemas%20de%20Informaci%C3%B3n%20ESI%202012-0.4.pdf?sequence=1&isAllowed=y

ALLSOPP, Wil. Advanced Penetration Testing: Hacking the World's Most Secure Networks. San Francisco: John Wiley & Sons, Incorporated. 2017. p.147. ISBN 9781119367680

ANTONUCCI. Domenic. The Cyber Risk Handbook: Creating and Measuring Effective Cybersecurity Capabilities. San Francisco: John Wiley & Sons, Incorporated. 2017. p.137. ISBN 9781119308805

ARGONNE. DarkNet Terminology: Definitions of the DarkNet, the Dark Web, and the Deep Web. [Sitio Web]. [Consulta: 22 de enero de 2021]. Disponible en: https://coar.risc.anl.gov/coar-attends-department-of-homeland-security-hosted-darknet-summit/

AVAST. ¿Qué es el spyware? [Sitio Web]. Patrick Seguin. [Consulta: 20 de enero de 2021]. Disponible en: https://www.avast.com/es-es/c-spyware

AVG Antivirus. Qué es el smishing y cómo evitarlo. [Sitio web]. Praga. Asher, Colin. [Consulta: 11 de mayo 2020]. Disponible en: https://www.avg.com/es/signal/what-is-smishing

BALBOA-ROMERO. Francisco José. Ransomware, hacking y phishing: conducta típica del delito de daños informáticos [en línea]. [Consulta: 22 de noviembre de 2020]. Disponible en: https://reunir.unir.net/bitstream/handle/123456789/6929/BALBOA%20ROMERO%2c%20FRANCISCO%20JOS%c3%89.pdf?sequence=1&isAllowed=y

BBC. Deepfakes: What are they and why would I make one? [Sitio Web]. [Consulta: 22 de enero de 2021]. Disponible en: https://www.bbc.co.uk/bitesize/articles/zfkwcqt

BBVA. 'Phishing', 'vishing', 'smishing', ¿qué son y cómo protegerse de estas amenazas? [Sitio web]. Madrid.: Castillo, Claudia. [Consulta: 15 de mayo 2020].

Disponible en: https://www.bbva.com/es/phishing-vishing-smishing-que-son-y-como-protegerse-de-estas-amenazas/

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias cibercrimen Colombia 2019-2020. Bogotá D.C. 2019. P.6.

CERT-UK. An introduction to social engineering. [Sitio web]. Londres. [Consulta: 14 de mayo 2020]. Disponible en: https://www.oodaloop.com/wp-content/uploads/2015/02/UKCERT-SocialEngineering.pdf

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3701. (14, Julio, 2011). Lineamientos de política para ciberseguridad y ciberdefensa. Bogotá D.C. 2009. p. 1-43.

--------. Documento Conpes 3854. (7, marzo, 2017). Política nacional de seguridad digital. Bogotá D.C. 2017. p. 1-2.

COLOMBIA. CONGRESO DE LA REPUBLICA, Ley 1273 (5, enero, 2009). "Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos". Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1-4.

--------. Ley 1928. (24, julio, 2018). Por medio de la cual se aprueba el «CONVENIO SOBRE LA CIBERDELINCUENCIA», Adoptado el 23 de noviembre de 2001, en Budapest. Diario Oficial. Bogotá, D.C., 2018. no. 50.664. p.1-49.

--------. Ley 599 (24, julio, 2000) Código Penal Colombiano. Diario Oficial. Bogotá, D.C. 2000. No. 44.097. p 1-428.

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

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

DAY, Graham. Security in the Digital World: For the home user, parent, consumer and home office. Londres: IT Governance Ltd, 2017. p.64. ISBN 9781849289610

Delitos en Internet: Clases de fraudes y estafas y las medidas para prevenirlos [en línea]. Madrid: Universidad Complutense de Madrid, 2012. [Fecha de consulta: 22 abril 2020]. Disponible en internet: https://dialnet.unirioja.es/descarga/articulo/4198948.pdf

DELTA ASESORES. Ley de Delitos Informáticos en Colombia. [Sitio web]. Bogotá. [Consulta: 5 de mayo 2020]. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

DIGICERT. Breve historia del phishing. [Sitio web]. Madrid. Digicert. [Consulta: 10 de mayo 2020]. Disponible en: https://www.websecurity.digicert.com/es/es/security-topics/brief-history-phishing-part-1

DINCA, Claudia Florentina. Fraudes en Internet [en línea]. Trabajo de grado. Universitat Jaume I. 2016. [Consultado 22 abril 2020]. Disponible en http://repositori.uji.es/xmlui/bitstream/handle/10234/161252/TFG_2016_DincaClaudia.pdf?sequence=1

DOLAN, Aaron, Social Engineering. [Sitio Web]. [Consulta: 1 de junio de 2021]. Disponible en: https://www.sans.org/reading-room/whitepapers/engineering/social-engineering-1365

EUROPOL. Fraude del CEO. [Sitio web]. The Hague: EUROPOL. [Consulta: 8 de abril 2020]. Disponible en: https://www.europol.europa.eu/sites/default/files/documents/colombia_1.pdf

ESCRIVÁ GASCO, Gema, et al. Seguridad informática. Madrid: MacMillan Iberia, 2013. p.7. ISBN 978-841-56-5664-7

GARCÍA GARCÍA, Diego Eloy, El phishing como delito de estafa informática. [En línea]. 2018, [Consultado 1 de mayo 2020]. Disponible en: https://dialnet.unirioja.es/servlet/articulo?codigo=6263417

GUERRERO, Diego, Fraude en la Red. Madrid. Ra-Ma Editorial. 2012. P.31. ISBN 9789587620665

GOGA, Oana; VENKATADRI, Giridhari y GUMMADI, Krishna P. Exposing Impersonation Attacks in Online Social Networks. [En línea]. 2016, [Consultado 1 de mayo 2020]. Disponible en: https://lig-membres.imag.fr/gogao/papers/impers_cosn14.pdf

HADNAGY, Christopher y WILSON, Paul, Ingeniería social: El arte de la piratería humana. New York. John Wiley & Sons, Incorporated, 2010. p.40. ISBN 9780470639535

HERNÁNDEZ DOMINGUEZ, Antonio, Sistema para la detección de ataques PHISHING utilizando correo electrónico. [Sitio web]. [Consulta: 10 de diciembre 2020]. Disponible en: https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/304

HORNET SECURITY. Bussiness email compromise. [Sitio web]. Hannover.: Kreyenberg. Hannah. [Consulta: 16 mayo 2020]. Disponible en: https://www.hornetsecurity.com/es/seguridad-de-la-informacion/business-email-compromise-bec-la-amenaza-crece-rapidamente/

HUNGRIA. CONSEJO DE EUROPA. (23, noviembre, 2001). Convenio sobre la ciberdelincuencia. Serie de tratados europeos. Budapest, Hungría. 2001. No. 185. P. 1-26.

INCIBE. OSINT - La información es poder. [Sitio web]. Madrid. [Consulta: 30 de abril 2020]. Disponible en: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

KASPERSKY. What is Spear Phishing? [en línea]. [Consulta: 23 de enero de 2021]. Disponible en: https://www.kaspersky.com/resource-center/definitions/spear-phishing

LÓPEZ GRANDE, Carlos Edgardo y SALVADOR GUADRÓN, Ricardo. Ingeniería Social: El Ataque Silencioso [en línea]. 2015, enero –diciembre, vol.7, nro.1. [Consultado 02 de mayo 2020]. ISSN 2072-568X. disponible en: http://www.redicces.org.sv/jspui/bitstream/10972/2910/1/Articulo6.pdf

MAILFENCE. Ingeniería Social: ¿qué es el Baiting («cebar», o «poner carnada»)? [Sitio web]. [Consulta: 10 de mayo 2020]. Disponible en: https://blog.mailfence.com/es/que-es-baiting-ingenieria-social/

--------. Ingeniería Social: ataques de Quid pro Quo. [Sitio web]. [Consulta: 10 de mayo 2020]. Disponible en: https://blog.mailfence.com/es/ataques-de-quid-pro-quo/

MARTÍNEZ SANTANDER, Carlos José. et al. Seguridad por capas frenar ataques de Smishing. Dominio de las ciencias [en línea] Manta - Manabí (Ecuador): Polo de Capacitación, Investigación y Publicación (POCAIP) 01 enero 2018, vol. 4, nro 1. [Consultado 6 abril 2020]. ISSN 2477-8818. Disponible en: https://dialnet.unirioja.es/descarga/articulo/6255067.pdf

Methods for Understanding and Reducing Social Engineering Attacks [en Línea]. Boston: SANS Institute Information Security Reading Room, 2016. [Fecha de consulta: 14 mayo 2020]. Disponible en: https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Guía para la implementación de seguridad de la información en una MIPYME. Bogotá
D.C. 2016. p.15.

MITNIK, Kevin y SIMON, William. El arte de la intrusión. Madrid: RA-MA Editorial, 2001. p.24. ISBN 978-970-15-1260-9

--------. The Art of Deception. Indianapolis: WILEY Publishing, Inc, 2001. p.350. ISBN 0-471-23712-4

NOHLBERG, Marcus, Securing Information Assets: Understanding, Measuring and Protecting against Social Engineering Attacks. Estocolmo. Universitetsservice US-AB. 2018. p.59. ISBN 978-91-7155-786-5

NORD VPN. How to identify and prevente vil twin attacks. [Sitio web]. Helsinki.: Green, Emily. [Consulta: 20 de mayo 2020]. Disponible en: https://nordvpn.com/es/blog/evil-twin-attack/

NORTON. What is vishing? Tips for spotting and avoiding voice scams. [Sitio Web]. [Consulta: 22 de enero de 2021]. Disponible en: https://us.norton.com/internetsecurity-online-scams-vishing.html

PC WORLD. Types of Phishing Attacks. [Sitio web]. California. Computer Associates. [Consulta: 20 de mayo 2020]. Disponible en: https://www.pcworld.com/article/135293/article.html

POLICÍA MUNICIPAL DE MADRID. Ingeniería social: ¿Se puede hackear a una persona? [Sitio web]. Madrid. [Consulta: 1 de mayo 2020]. Disponible en: https://cppm.es/wp-content/uploads/2019/03/ingenieria-social-se-puede-hackear-a-una-persona-abr2019.pdf

POLICÍA NACIONAL DE COLOMBIA. Amenazas del cibercrimen en Colombia 2016-2017. Bogotá D.C.: Ministerio de Defensa Nacional, 2017. P.10.

--------. Balance cibercrimen en Colombia 2017. Bogotá D.C.: Ministerio de Defensa Nacional, 2017. P.6.

PONS GAMÓN. A. Vicente. Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. [en línea]. [Consulta: 22 de enero de 2021]. Disponible en: https://www.redalyc.org/jatsRepo/5526/552656641007/index.html

Portafolio. Conozca las formas de fraude en la web: Los delitos informáticos más comunes en las compañías son ‘phishing’, ‘ransomware’ y ‘malware’. [en línea].

[Consulta: 22 de octubre de 2020]. Disponible en: https://bv.unir.net:2257/docview/2295404820/fulltext/582DFCC6177741A0PQ/1?accountid=142712

--------. Guía para no ser víctima de correos maliciosos: En esta época los casos de phishing se han incrementado. Conozca cómo identificar el engaño y qué puede hacer si le llega un correo sospechoso. [en línea]. [Consulta: 22 de octubre de 2020]. Disponible en: https://bv.unir.net:2257/docview/2436363867?pq-origsite=summon

Revista de Derecho [en línea]. Valparaíso: Pontificia Universidad Católica de Valparaíso, 2016. [Fecha de consulta: 22 abril 2020]. Disponible en internet: https://scielo.conicyt.cl/pdf/rdpucv/n41/a07.pdf

SÁNCHEZ, Joana. Tecnología pyme - Weblogs SL: Los casos de 'phishing' se ceban con los nuevos teletrabajadores. [en línea]. [Consulta: 22 de octubre de 2020]. Disponible en: https://bv.unir.net:2257/docview/2394653412?pq-origsite=summon

SECURECLICK. Glosario de términos de ingeniería social y seguridad de la información de AZ. [Sitio Web]. [Consulta: 22 de enero de 2021]. Disponible en: https://www.itsecurityawareness.ie/a-z-glossary-of-information-security-and-social-engineering-terms

SERRATO BERENGUER, David. Estudio de metodologías de Ingeniería Social [en línea] Trabajo fin de Máster. Universitat Oberta de Catalunya, 2018. [Consultado 14 abril 2020]. Disponible en: http://openaccess.uoc.edu/webapps/o2/bitstream/10609/81273/6/dbs14TFM0618memoria.pdf

TECHTARGET. Whaling attack (whaling phishing). [Sitio Web]. [Consulta: 20 de enero de 2021]. Disponible en: https://searchsecurity.techtarget.com/definition/whaling

--------. Watering hole attack. [Sitio web]. San Francisco. [Consulta: 05 de mayo 2020]. Disponible en: https://searchsecurity.techtarget.com/definition/watering-hole-attack

THOMAS, Douglas. Hacker Culture. Minnesota: University of Minnesota Press, 2002. P .90. ISBN 978-081-66-3345-6

TOLMAN, William Howe. Social Engineering. Charleston: BiblioBazaar Publisher, 2010. p.4. ISBN 978-05-5933-064-3

TREND MICRO. Smishing. [Sitio Web]. [Consulta: 22 de enero de 2021]. Disponible en: https://www.trendmicro.com/vinfo/us/security/definition/smishing

ANEXOS

ANEXO A. Resumen Analítica Especializado -RAE

Fecha de Realización:	14/02/2021
Programa:	ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
Línea de Investigación:	
Título:	IMPACTO DE LOS ATAQUES DE INGENIERÍA SOCIAL EN COLOMBIA DESDE EL AÑO 2016 HASTA EL AÑO 2019.
Autor(es):	PAOLA MARITZA RINCÓN NUÑEZ
Palabras Claves:	Engaño, estafa, ataque, ciber-delincuente, Phishing.
Descripción:	Para lograr analizar el impacto de los ataques de ingeniería social en Colombia desde el año 2016 hasta el año 2019, se debe realizar una breve descripción de la terminología relacionada a la Ingeniera social, normativa, legislación y conceptos; logrando concluir cuáles son las técnicas de ingeniería social más utilizadas y que afectan a la población colombiana. Otro aspecto importante es identificar si existen estrategias o campañas por parte de las entidades del estado, para contribuir a mitigar la ocurrencia de incidentes relacionados o producidos. Se puede lograr que la ciudadanía, los entes gubernamentales y las empresas, identifiquen el tema como una problemática socioeconómica, que puede afectar desde su entorno familiar y laboral de las personas, o la empresa en general, y así se logre implementar a nivel educativo términos fundamentales de ingeniería social y poder mitigar la brecha de la inseguridad por la ejecución de dichas técnicas, aprovechando las falencias del ser humano, que por naturaleza es confiado. El propósito fundamental es obtener un conjunto de buenas prácticas y recomendaciones para que las personas no se vean afectadas por ataques de ingeniería social, para que posteriormente las organizaciones las puedan utilizar para realizar la

	concienciación del personal y como estrategia de prevención.

Fuentes bibliográficas destacadas:

ACENS TECHNOLOGIES. Qué es el phishing y cómo protegerse. [Sitio web]. Madrid: Telefónica. [Consulta: 15 de abril 2020]. Disponible en: https://www.acens.com/wp-content/images/2014/10/wp-phising-acens.pdf

AENOR. Seguridad en Sistemas de Información Un recorrido a vista de pájaro. [Sitio web]. Ciudad Real. [Consulta: 1 de mayo 2020]. Disponible en: https://ruidera.uclm.es/xmlui/bitstream/handle/10578/2302/Seguridad%20en%20Sistemas%20de%20Informaci%C3%B3n%20ESI%202012-0.4.pdf?sequence=1&isAllowed=y

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias cibercrimen Colombia 2019-2020. Bogotá D.C. 2019. P.6.

CERT-UK. An introduction to social engineering. [Sitio web]. Londres. [Consulta: 14 de mayo 2020]. Disponible en: https://www.oodaloop.com/wp-content/uploads/2015/02/UKCERT-SocialEngineering.pdf

COLOMBIA. DEPARTAMENTO NACIONAL DE PLANEACIÓN. Documento Conpes 3701. (14, Julio, 2011). Lineamientos de política para ciberseguridad y ciberdefensa. Bogotá D.C. 2009. p. 1-43.

--------. Documento Conpes 3854. (7, marzo, 2017). Política nacional de seguridad digital. Bogotá D.C. 2017. p. 1-2.

COLOMBIA. CONGRESO DE LA REPUBLICA, Ley 1273 (5, enero, 2009). "por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos". Diario Oficial. Bogotá, D.C., 2009. no. 47223. p. 1-4.

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

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

Delitos en Internet: Clases de fraudes y estafas y las medidas para prevenirlos [en línea]. Madrid: Universidad Complutense de Madrid, 2012. [Fecha de consulta: 22 abril 2020]. Disponible en internet: https://dialnet.unirioja.es/descarga/articulo/4198948.pdf

DELTA ASESORES. Ley de Delitos Informáticos en Colombia. [Sitio web]. Bogotá. [Consulta: 5 de mayo 2020]. Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

DIGICERT. Breve historia del phishing. [Sitio web]. Madrid. Digicert. [Consulta: 10 de mayo 2020]. Disponible en: https://www.websecurity.digicert.com/es/es/security-topics/brief-history-phishing-part-1

EUROPOL. Fraude del CEO. [Sitio web]. The Hague: EUROPOL. [Consulta: 8 de abril 2020]. Disponible en: https://www.europol.europa.eu/sites/default/files/documents/colombia_1.pdf

ESCRIVÁ GASCO, Gema, et al. Seguridad informática. Madrid: MacMillan Iberia, 2013. p.7. ISBN 978-841-56-5664-7

GOGA, Oana; VENKATADRI, Giridhari y GUMMADI, Krishna P. Exposing Impersonation Attacks in Online Social Networks. [En línea]. 2016, [Consultado 1 de mayo 2020]. Disponible en: https://lig-membres.imag.fr/gogao/papers/impers_cosn14.pdf

HADNAGY, Christopher y WILSON, Paul, Ingeniería social: El arte de la piratería humana. New York. John Wiley & Sons, Incorporated, 2010. p.40. ISBN 9780470639535

HORNET SECURITY. Bussiness email compromise. [Sitio web]. Hannover.: Kreyenberg. Hannah. [Consulta: 16 mayo 2020]. Disponible en: https://www.hornetsecurity.com/es/seguridad-de-la-informacion/business-email-compromise-bec-la-amenaza-crece-rapidamente/

HUNGRIA. CONSEJO DE EUROPA. (23, noviembre, 2001). Convenio sobre la ciberdelincuencia. Serie de tratados europeos. Budapest, Hungría. 2001. No. 185. P. 1-26.

INCIBE. OSINT - La información es poder. [Sitio web]. Madrid. [Consulta: 30 de abril 2020]. Disponible en: https://www.incibe-cert.es/blog/osint-la-informacion-es-poder

LÓPEZ GRANDE, Carlos Edgardo y SALVADOR GUADRÓN, Ricardo. Ingeniería Social: El Ataque Silencioso [en línea]. 2015, enero –diciembre, vol.7, nro.1. [Consultado 02 de mayo 2020]. ISSN 2072-568X. disponible en: http://www.redicces.org.sv/jspui/bitstream/10972/2910/1/Articulo6.pdf

MAILFENCE. Ingeniería Social: ¿qué es el Baiting («cebar», o «poner carnada»)? [Sitio web]. [Consulta: 10 de mayo 2020]. Disponible en: https://blog.mailfence.com/es/que-es-baiting-ingenieria-social/

--------. Ingeniería Social: ataques de Quid pro Quo. [Sitio web]. [Consulta: 10 de mayo 2020]. Disponible en: https://blog.mailfence.com/es/ataques-de-quid-pro-quo/

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE COLOMBIA. Guía para la implementación de seguridad de la información en una MIPYME. Bogotá
D.C. 2016. p.15.

MITNIK, Kevin y SIMON, William. El arte de la intrusión. Madrid: RA-MA Editorial, 2001. p.24. ISBN 978-970-15-1260-9

--------. The Art of Deception. Indianapolis: WILEY Publishing, Inc, 2001. p.350. ISBN 0-471-23712-4

NORD VPN. How to identify and prevente vil twin attacks. [Sitio web]. Helsinki.: Green, Emily. [Consulta: 20 de mayo 2020]. Disponible en: https://nordvpn.com/es/blog/evil-twin-attack/

POLICÍA NACIONAL DE COLOMBIA. Amenazas del cibercrimen en Colombia 2016-2017. Bogotá D.C.: Ministerio de Defensa Nacional, 2017. P.10.

--------. Balance cibercrimen en Colombia 2017. Bogotá D.C.: Ministerio de Defensa Nacional, 2017. P.6.

THOMAS, Douglas. Hacker Culture. Minnesota: University of Minnesota Press, 2002. P .90. ISBN 978-081-66-3345-6

TOLMAN, William Howe. Social Engineering. Charleston: BiblioBazaar Publisher, 2010. p.4. ISBN 978-05-5933-064-3

Contenido del documento:	1. INTRODUCCIÓN 1. DEFINICIÓN DEL PROBLEMA 1.1 ANTECEDENTES DEL PROBLEMA 1.2 FORMULACIÓN DEL PROBLEMA 2. JUSTIFICACIÓN

	3. OBJETIVOS 3.1 OBJETIVOS GENERAL 3.2 OBJETIVOS ESPECÍFICOS 4. MARCO REFERNCIAL 4.1 MARCO TEÓRICO 4.1.1 Phishing. 4.1.2 Smishing. 4.1.3 Vishing. 4.1.4 Impersonation. 4.2 MARCO CONCEPTUAL 4.2.1 Spear phishing. 4.2.2 Baiting. 4.2.3 Watering hole attack. 4.2.4 Quid pro quo. 4.3 MARCO LEGAL 37 5. DESARROLLO DE LOS OBJETIVOS 5.1 Origen y evolucion de los ataques de ingenieria social 5.1.1 Phishing general. Phishing tradicional, Bulk Phishing o Spray and pray. 5.1.2 Vishing. 5.1.3 Smishing. 5.1.4 URL Phishing. 5.1.5 Whaling. 5.1.6 Business Email Compromise (BEC) o estafas Man-in-the-Email. 5.1.7 CEO Fraud. 5.1.8 Spear Phishing. 5.1.9 Search Engine phishing. 5.1.10 Phising con evasión de filtros. 5.1.11 Pharming o DNS-Based Phishing. 5.1.12 Malware-based phishing. 5.1.13 Content-Injection phishing. 5.1.14 Watering Hole Phishing, watering hole attack. 5.1.15 Evil Twin. 5.1.16 Social Network Phishing. 5.1.17 Phishing 2.0. 5.1.18 Hishing o “hardware phishing”. 5.2 Evolución de la ingeniería social 5.3 Ataques de ingeniería social más utilizados en Colombia

	5.4 Estrategias propuestas por parte de las entidades del estado colombiano para la mitigación de los ataques de ingeniería social. 5.5 Buenas prácticas y recomendaciones para que las personas no se vean afectadas por ataques de ingeniería social. 5.5.1 Estafa. 5.5.2 Phishing. 5.5.3 Suplantación. 5.5.4 Vishing. 5.5.5 Smishing. 5.5.6 Carta nigeriana. 6. CONCLUSIONES 7. RECOMENDACIONES BIBLIOGRAFÍA ANEXOS
Marco Metodológico:	La presente investigación se desarrolla con una metodología exploratoria-descriptiva, a partir de la recolección y revisión de información se profundizará en el tema de estudio IMPACTO DE LOS ATAQUES DE INGENIERÍA SOCIAL EN COLOMBIA DESDE EL AÑO 2016 HASTA EL AÑO 2019 y de cómo esto ha afectado a los usuarios colombianos, esto permite realizar el análisis descriptivo, y definir las características específicas de este tipo de amenaza. Inicialmente se realiza la recopilación de la información, la revisión bibliográfica de datos proporcionados por entes gubernamentales y empresas de seguridad informática. Posteriormente, se realiza un compilado de todas las medidas que se han tomado para prevenir este tipo de incidentes para finalmente proponer un conjunto de buenas prácticas para prevenir ataques de ingeniería social.
Conceptos adquiridos:	BUENAS PRÁCTICAS Y RECOMENDACIONES PARA QUE LAS PERSONAS NO SE VEAN AFECTADAS POR ATAQUES DE INGENIERÍA SOCIAL. De acuerdo con el análisis realizado, en Colombia se mantiene la tendencia en el periodo de 2016 a 2019 por parte de los ciberdelincuentes el uso de técnicas relacionadas a la Ingeniería Social, de tal

	forma que se identifican 6 modalidades que representan un riesgo para los usuarios de internet en nuestro país. Por lo tanto, se proponen unas buenas prácticas y recomendaciones para que las personas no se vean afectadas por ataques de este tipo.
Conclusiones:	• Los ataques de ingeniería social han evolucionado de tal forma que cada vez es mucho más complicado para los usuarios identificar este tipo de amenazas, desde los inicios de internet se han conocido casos de ataques de este tipo, y a pesar de esto aún los delincuentes hacen uso de las mismas técnicas, pero incorporando nuevas tecnologías para engañar a las personas. • El ciber crimen en Colombia, ha tenido un crecimiento exponencial durante los últimos años de forma paralela al uso de las nuevas tecnologías y acceso a dispositivos móviles. Las pérdidas económicas generadas por los ciberataques asociados a la ingeniería social sitúan a esta problemática como una de las principales actividades ilegales en el País. • Para los atacantes la ingeniería social se ha convertido en su primera opción al momento de ejecutar un ataque, puesto que gracias a los diferentes métodos y técnicas se logra obtener mayor efectividad. Como se logra identificar es una problemática real y es prioritario tomar medidas al respecto. • La cantidad de delitos informáticos que son denunciados en Colombia como fue posible evidenciar son bastantes, pero el escenario que más preocupa es el aumento desde el año 2016 y que no todas las victimas denuncian la ocurrencia de este tipo de eventos. • Al aprovechar las debilidades humanas naturales, las estafas del tipo phishing continúan siendo un tipo de ataque común y eficaz, ya que su porcentaje de éxito radica en que el atacante envía miles de correos y al afectar un pequeño

	grupo de estos puede obtener el beneficio económico. Es importante contar con un software antivirus, toda vez que cumplen un rol importante que desempeñar en la prevención de ataques de phishing, pero el usuario debe asegurarse que su antivirus realmente combate el phishing y los riesgos de seguridad y privacidad que esto implica. • Toda organización cuenta con el factor humano, por lo tanto, los humanos, por naturaleza, es curioso, propenso a tomar decisiones de manera rápida y, con frecuencia, están guiados por las emociones. Por esta razón, es fundamental que desarrolle un conjunto de herramientas de ingeniería social para contribuir a reforzar la seguridad contra los ataques de este tipo que normalmente aprovechan las vulnerabilidades humanas.