ESTUDIO SOBRE LA INGENIERÍA SOCIAL Y SU IMPACTO EN LAS ENTIDADES ESTATALES

MARVER ALBERTO BASTO GARCÍA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA, SANTANDER
2020

ESTUDIO SOBRE LA INGENIERÍA SOCIAL Y SU IMPACTO EN LAS ENTIDADES ESTATALES

MARVER ALBERTO BASTO GARCÍA

Monografía para optar al título de
Especialista en Seguridad Informática

Director
Ingeniero Eduard Antonio Mantilla Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BUCARAMANGA, SANTANDER
2020

Nota de Aceptación

_____
_____
_____
_____
_____

_____
Firma Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bucaramanga, mayo, 2020

Dedicatoria

Este proyecto es dedicado a mi familia que ha sido el motor de mi vida, porque he alcanzado muchos triunfos y logros gracias al acompañamiento, apoyo y dedicación que me han bridado.

A Dios también dedico este logro pues ha sido mi guía espiritual y compañero que ha estado en todo momento durante el camino que he recorrido.

Agradecimientos

Este proyecto monográfico realizado como requisito para optar a especialista de la Universidad Nacional Abierta y a Distancia, es el acompañamiento de varias personas que confiaron en mí para la elaboración del mismo.

Al Ingeniero Eduard Antonio Mantilla Torres por su paciencia y dirección en la realización de este proyecto, así mismo con el asesoramiento para realizar las mejoras indicadas al documento con el propósito de dar la culminación del proyecto.

A mis compañeros de curso, por sus observaciones en cada una de las fases en que fue compartido el documento y por la participación en sus apreciaciones.

CONTENIDO

pág.

LISTA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

BAITING: en esta técnica los delincuentes utilizan USB con software malicioso. Con el fin de que la víctima realice la conexión de estos dispositivos, se hace un estudio en el comportamiento de la persona previamente.

DUMPSTER DIVING: la utilizan los delincuentes para registrar o revisar la basura, debido a que en ocasiones se arrojan documentos con información sensible (usuarios, contraseñas, entre otros) en las Entidades y que no son destruidos en su totalidad por los empleados y la cual los delincuentes la utilizan para fines fraudulentos.

PHISHING: esta técnica busca víctimas a través del envío de correos electrónicos, los cuales contienen malware o links a páginas clonadas o falsas, es decir páginas que son parecidas a las reales (Entidades Bancarias, comercio para compras con tarjetas de crédito, recolección de dineros para donaciones solidarias, entre otras.) con el fin de robar las credenciales ingresadas por las víctimas.

PRETEXTING: los delincuentes en este tipo de ataques se hacen pasar por empleados que laboran en la misma Entidad, por ejemplo, del área técnica y que le indica a la víctima que el PC que usa presenta una anomalía que debe ser revisada, de esta manera le facilita la instalación de algún tipo de malware con el fin de tomar control del equipo para obtener información.

REDES SOCIALES: en esta técnica los delincuentes buscan no solamente obtener una relación cercana con la víctima, sino también obtener información generando confianza, debido a que las personas tienden a dar a conocer toda su vida personal en estas redes.

SHOULDER SURFING: esta técnica es utilizada para espiar a las personas por encima del hombro, con el fin de obtener contraseñas, patrones o códigos que son utilizados en equipos o teléfonos celulares, las cuales puedan ingresar a estos dispositivos que contienen información sensible.

SMISHING (SMS): esta técnica es utilizada mediante los teléfonos celulares, en la cual los delincuentes envían un mensaje de texto indicando a la víctima que ha ganado un premio, ya sea mediante un link, devolver la llamada a un número telefónico o responder un sms.

SPEAR PHISHING: en esta técnica se utilizan los correos electrónicos dirigidos a empleados con perfiles determinados, es decir que tienen acceso a sistemas informáticos dentro de una Entidad u Organización, a fin de que sean ellos quienes suministren información interna.

TAILGAITING: este tipo de técnica, es utilizado cuando existe una restricción de acceso físico en una Entidad (tarjeta de ingreso, etc), por tanto, el delincuente se aprovecha de la víctima a través de la buena voluntad y le indica que no trajo o se le olvido la tarjeta o dispositivo para ingresar, de esta manera manipula a la víctima para ingresar a la Entidad.

VISHING: en esta técnica se instauran falsos centros de atención telefónica que realizan llamadas con el propósito de efectuarse un fraude, es decir consiste en el robo de credenciales bancarias utilizando VoIP (Voice over IP).

RESUMEN

El crecimiento de la tecnología a nivel mundial ha permitido que las empresas tengan la necesidad de implementar más recursos tecnológicos, los cuales buscan la optimización de los procesos al interior de las mismas; a su vez dicho crecimiento conllevó la generación de delitos informáticos desarrollados por delincuentes informáticos que aprovechan las vulnerabilidades que tienen algunas organizaciones.

De esta forma la Ingeniería Social utiliza el método de engañar a una persona con el fin de sustraer información o acceder a un sistema de información, por lo tanto en la actualidad no importa el nivel de seguridad de una empresa o que tan seguro es un sistema de información, ya que con el hecho de una persona esté a cargo o controle una área específica, estará vulnerable a un ataque mediante la ingeniería social, por esta razón, es necesario establecer una serie de acciones, las cuales permitan evitar estos posibles ataques al interior de las mismas.

Todos los ataques de ingeniería social dependen de que la víctima confíe en el atacante y le otorgue información o datos o acceso. Se ha demostrado que las personas se desempeñan mal en la detección de mentiras y engaños y generalmente sobreestiman sus capacidades de detección. Los usuarios humanos, que son el eslabón más débil en la cadena de seguridad de la información, siguen siendo susceptibles de ser manipulados por los ingenieros sociales.

Es por ello, que con el desarrollo de este documento se propone un Plan de Acción que posterior a su implementación dará como resultado recomendaciones, las cuales permitan contrarrestar los posibles ataques informáticos basados en ingeniería social a nivel Gobierno, y de esta manera las entidades puedan implementar mayor control en la seguridad de la información al interior de las mismas, resaltando que dichas recomendaciones van de la mano con políticas de seguridad de la información las cuales deberán ser diseñas e implementadas por cada una de las organizaciones del estado.

PALABRAS CLAVES: Ingeniería Social, seguridad de la información, gobierno, delitos informáticos, delincuentes informáticos.

ABSTRACT

The growth of technology worldwide has allowed companies to have the need to implement more technological resources, which seek to optimize processes within them; In turn, this growth led to the generation of computer crimes developed by computer criminals who take advantage of the vulnerabilities of some organizations.

In this way, Social Engineering uses the method of deceiving a person in order to subtract information or access an information system, therefore currently it does not matter the level of security of a company or how safe a system is of information, since with the fact of a person being in charge or controlling a specific area, he will be vulnerable to an attack through social engineering, for this reason, it is necessary to establish a series of actions, which allow these possible attacks to be avoided inside of them.

All social engineering attacks depend on the victim trusting the attacker and granting him information or data or access. It has been shown that people perform poorly in detecting lies and deceptions and generally overestimate their detection abilities. Human users, who are the weakest link in the information security chain, remain susceptible to being manipulated by social engineers.

That is why, with the development of this document, an Action Plan is proposed that, after its implementation, will result in recommendations, which will allow counteracting the possible attacks on social engineering based at the Government level, and in this way the entities can Implement greater control in information security within them, highlighting that these recommendations go hand in hand with information security policies which should be designed and implemented by each of the state organizations.

KEY WORDS: Social Engineering, information security, government, computer crimes, cybercriminals.

INTRODUCCIÓN

La ingeniería social se refiere en general a la manipulación psicológica del comportamiento humano que hace que las personas actúen de ciertas maneras o divulguen información confidencial. Es una técnica que explota nuestros prejuicios cognitivos e instintos básicos (por ejemplo, la confianza) con el propósito de recopilar información, fraude o acceso al sistema. A veces denominada "piratería humana", la ingeniería social es una herramienta favorita de los hackers en todo el mundo. Si bien esto se practicó históricamente cara a cara, por teléfono o por escrito, la ingeniería social ahora puede ocurrir en escalas sociales a través de las redes sociales y otras plataformas de Internet.

La ingeniería social se considera por los expertos como el ataque informático que genera mayor peligro, puesto que la información que es susceptible a estos ataques, es aquella que es usada diariamente por el factor humano.

El comportamiento de los empleados tiene un grave impacto en la ciberseguridad organizacional, lo que significa, por extensión, que la ingeniería social también lo hace. Las formas en que se enmarca y educa a los empleados sobre ciberseguridad impactan fundamentalmente la ciberseguridad misma. Aprovechar los conceptos culturales puede ayudar a diferentes segmentos de una organización a trabajar hacia la seguridad efectiva de la información, al igual que diseñar educación para los sesgos cognitivos humanos. Estos principios caen bajo el concepto de una cultura de seguridad de la información, definida como la totalidad de los patrones de comportamiento que contribuyen a la protección de la información de una organización.

Es así que las Organizaciones y Entidades se preocupan principalmente por mantener controles en los Sistemas de Información y de esta manera evitar la sustracción y manipulación de la misma, pero se olvidan de capacitar y preparar al personal, lo cual genera vulnerabilidades, que los criminales aprovechan para entrar a los sistemas informáticos. Parte de una cultura de seguridad requiere una conciencia de la ingeniería social. Comprender que los piratas informáticos intentan manipular activamente el comportamiento es esencial para la gestión diaria de riesgos y el desarrollo de "instintos" cibernéticos. Cuando los empleados no se ven a sí mismos como parte de este esfuerzo, actuarán de manera que solo se ignoren la seguridad en pro de sus propios intereses.

Por tales motivos es ineludible que la Entidades creen conciencia y puedan conocer cuáles son las técnicas que utilizan los criminales en dichos fines fraudulentos,

adicionalmente es necesario que se creen políticas al interior de las mismas, toda vez que al ser Entidades Estatales manejan información pública que puede ser alterada fácilmente.

De acuerdo con lo anterior, surge la necesidad de investigar sobre la Ingeniería Social y las causas más relevantes que se presentan en los últimos años y de esta manera evitar riesgos que se materialicen por la falta de seguimiento y controles suficientes, logrando con ello impedir perdidas de dinero, imagen, credibilidad y sobre todo que afecten otros activos de las Entidades del Estado.

Como resultado de esta investigación se pretende generar un plan de acción, que ayude a las Entidades a seguir una ruta que les permita evitar ser víctimas de ataques de Ingeniería Social.

1. DEFINICIÓN DEL PROBLEMA

1.1 DESCRIPCIÓN DEL PROBLEMA

Dentro de los avances tecnológicos generados en los últimos años, como es el uso de nuevos elementos de seguridad cibernética, servidores en la nube entre otros, han traído consigo beneficios y desventajas tanto a las Organizaciones, Gobiernos y personas.

Es por tanto que los beneficios, se pueden apreciar ante la facilidad en la comunicación a través del uso de las TIC, puesto que es posible conectarse desde cualquier lugar del mundo en tiempo real sin importar las distancias de territorio, y gracias a estos cambios, se evidencia la diversidad de formas en que se muestra la información, así como la manera en que se prestan los servicios al ciudadano; ha contribuido a mejorar su calidad de vida, sin embargo, pese a todas las ventajas del uso de dichas herramientas, también existen desventajas, se han presentado problemas relacionados con ataques informáticos que son aprovechados por vulnerabilidades ya sea del propio sistema o por las personas que interactúan con la información de las Entidades u Organizaciones.

En una forma más explícita, en términos de riesgos de seguridad de la información, es por ello que recientemente, la investigación sobre seguridad de la información se ha expandido desde su orientación puramente tecnológica hasta su esfuerzo por comprender y explicar el papel del comportamiento humano en las violaciones de seguridad. Sin embargo, esta área ha carecido de estudios empíricos basados en la teoría es en los ataques de ingeniería social. Si bien existe una gran cantidad de literatura anecdótica, los factores que explican el éxito del ataque siguen siendo en gran medida especulativos, puesto que en su mayoría son generadas en su mayoría por la factor humano[1][2], prueba de ello se encuentran informes que explican cómo es el caso del informe Comprensión de la seguridad de la nube de la empresa de ciberseguridad, que desde los beneficios de adopción hasta las amenazas e inquietudes, el informe arroja luz sobre el hecho de que el 90 por ciento de las violaciones de datos corporativos en la nube ocurren debido a ataques de ingeniería social que atacan a los empleados de los clientes y no debido a problemas causados por sus proveedores de la nube, esto afirma que el factor humano es considerado como un elemento débil debido a que aún no comprende la importancia del manejo de la información ya sea de Entidades estatales u Organizaciones privadas, puesto que los empleados o servidores públicos son quienes comparten o divulgan

[1] BYTE TI. La importancia y el riesgo del factor humano en la ciberseguridad. [En línea]. Madrid. 2017. Disponible en internet:<https://www.revistabyte.es/publirreportaje/riesgo-factor-humano-la-ciberseguridad/>.

[2] SPADAFORA A. El 90 por ciento de las violaciones de datos son causadas por un error humano. Artículo. En línea. 2019. Disponible en: https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error

información personal o confidencial sin darse cuenta, esta manipulación psicológica o persuasión realizada por un tercero, se conoce como INGENIERÍA SOCIAL[3]. Los ataques generalmente se perpetran en las redes sociales, o a través de técnicas como Phishing, Vishing, Baiting, entre otros, debido a que allí encuentran información sensible para ser utilizada para fines fraudulentos.

Es por ello que los avances en la tecnología de comunicación digital han hecho que la comunicación entre humanos sea más accesible e instantánea. Sin embargo, la información personal y confidencial puede estar disponible en línea a través de redes sociales y servicios en línea que carecen de las medidas de seguridad para proteger esta información. Los sistemas de comunicación son vulnerables y pueden ser fácilmente penetrados por usuarios maliciosos a través de ataques de ingeniería social. Estos ataques tienen como objetivo engañar a las personas o empresas para que realicen acciones que beneficien a los atacantes o les brinden datos confidenciales, como el número de seguro social, los registros de salud y las contraseñas. La ingeniería social es uno de los mayores desafíos que enfrenta la seguridad de la red porque explota la tendencia humana natural a confiar.

De igual forma, en la primera mitad de 2018 surgieron varias tendencias importantes de violación de datos. El más notable de estos desarrollos fue la introducción de nuevas regulaciones de protección de datos que incluyen el RGPD de la Unión Europea, los Requisitos de Ciberseguridad de Nueva York para las Empresas de Servicios Financieros y el esquema NDB de Australia. La razón fundamental para aprobar estos estándares es ayudar a las organizaciones a proteger mejor la privacidad y seguridad de los clientes por diseño. Vea nuestra infográfica del índice de nivel de incumplimiento a continuación para obtener estadísticas alarmantes de la primera mitad de 2018.[4]

Gemalto, el líder mundial en seguridad digital, lanzó los últimos hallazgos del Breach Level Index, una base de datos global de violaciones de datos públicos, que revela que 944 violaciones de datos llevaron a 3.300 millones de registros de datos comprometidos en todo el mundo en el primer semestre de 2018. En comparación con el mismo período en 2017, el número de registros perdidos, robados o comprometidos aumentó en un asombroso 72 por ciento, aunque el número total de infracciones disminuyó ligeramente durante el mismo período, lo que indica un aumento en la gravedad de cada uno incidente.[5]

---

[3] MINTIC. Ingeniería Social. [En línea]. Bogotá D.C. S.F. Disponible en internet:<http://www.mintic.gov.co/portal/604/w3-article-18800.html>.

[4] Gemalto. Incumplimientos de datos comprometidos 3.3 mil millones de registros en la primera mitad de 2018. Artículo. En línea. Disponible en: https://www.gemalto.com/press/pages/data-breaches-compromised-3-3-billion-records-in-first-half-of-2018.aspx

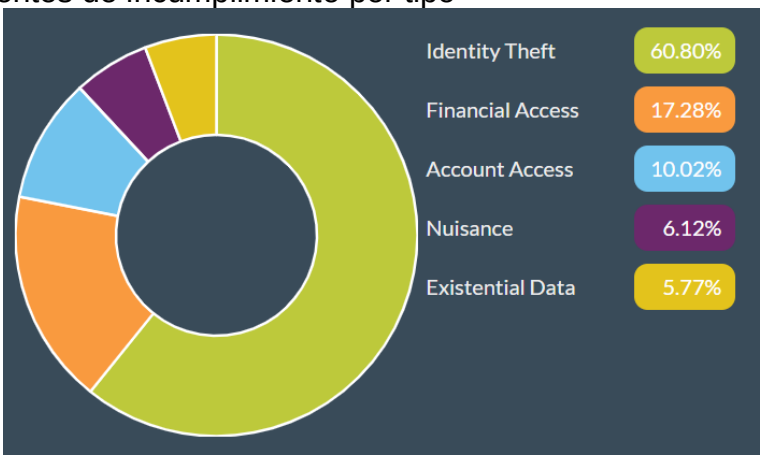
[5] Ibíd.

Un total de seis violaciones de redes sociales, incluido el incidente Cambridge Analytica-Facebook, representaron más del 56 por ciento del total de registros comprometidos. De las 944 violaciones de datos, 189 (20 por ciento de todas las violaciones) tenían un número desconocido o no contabilizado de registros de datos comprometidos.

Con base con lo anterior, se puede inferir que estos ataques han traído grandes pérdidas y han generado impactos irreparables a nivel de Gobierno en las Entidades Estatales, Organizaciones, y personas; según los hallazgos del índice de Breach Level realizado por el líder mundial en seguridad digital GEMALTO desde la vigencia 2013 al 2018.

Dichos hallazgos se pueden observar en la siguiente información por tipo, origen, industria, donde el porcentaje más alto por tipo se evidencia en el robo de identidad (Identity Theft), como se observa en la figura 1, con el 60.80% de todas las infracciones de datos por tipo.

Figura 1. Incidentes de incumplimiento por tipo

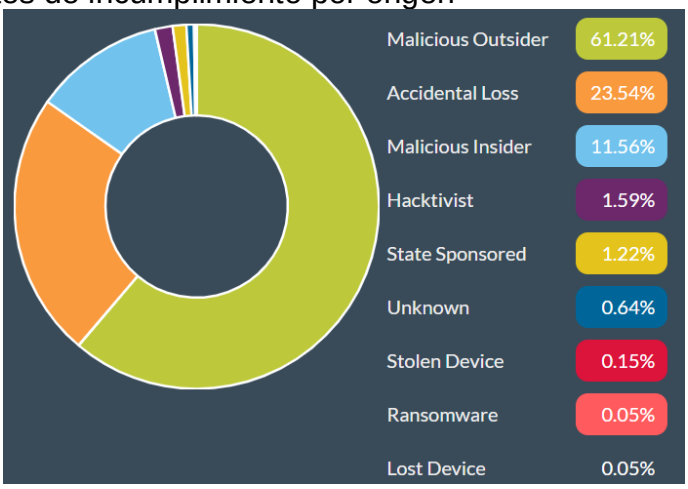


Fuente: GEMALTO. Breach Level Index. [En línea]. Disponible en internet: http://breachlevelindex.com/

Se ha visto un enorme aumento en los estudios relacionados con la ingeniería social. Este aumento se debe en parte al creciente número de ataques de ingeniería social y en parte a la incapacidad de las personas para identificar el ataque. Por lo tanto, es de gran importancia encontrar soluciones que sean útiles para que los humanos comprendan los ataques y escenarios de ingeniería social. Para abordar esto, se realiza una revisión de la literatura de estudios (sobre ingeniería social) en revistas y conferencias de primer nivel. Se puede lograr una mejor comprensión de los escenarios de ataque de ingeniería social utilizando técnicas de análisis temáticas y basadas en juegos. La evaluación empírica preliminar del método basado en el juego propuesto muestra resultados neutrales generales. Se necesita una extensión y evaluación futuras para los métodos propuestos.

En relación a los incidentes de incumplimiento por origen, el intruso malicioso (Malicious Outsider) presenta un 61.21% con el porcentaje más alto frente a la perdida accidental de información (Accidental Loss) con un 23.54% y la información privilegiada maliciosa (Malicious Insider) con un 11.56%, como se aprecia en la figura 2.

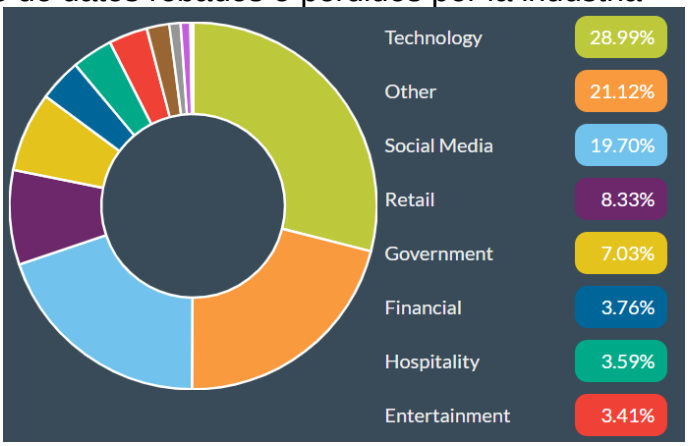
Figura 2. Incidentes de incumplimiento por origen



Fuente: GEMALTO. Breach Level Index. [En línea]. Disponible en internet: http://breachlevelindex.com/

Para la información referente a nivel de industria o sector, el mayor registro de datos robados o perdidos es a nivel de tecnología (Technology) con un 28.99% frente al nivel gobierno el cual es de 7.03%, siendo un porcentaje alto en comparación al sector financiero que es de 3.76% como se evidencia en la figura 3, esta información resalta que el sector gobierno está entre las principales industrias afectadas por los cibercriminales.

Figura 3. Registro de datos robados o perdidos por la industria



Fuente: GEMALTO. Breach Level Index. [En línea]. Disponible en internet: http://breachlevelindex.com/

Pese a que Internet está ayudando a personas de ideas afines a conectarse, comunicarse, compartir y difundir su punto de vista, sin embargo, en esta era digital en la que conectarse con las personas no es un problema, los atacantes también tienen acceso a un público más amplio mientras permanecen en el anonimato. Los ingenieros sociales, los extremistas y otros actores negativos de la sociedad están usando internet para difundir propaganda, conspiraciones e ideologías.

Teniendo en cuenta las cifras anteriormente expuestas, se puede sugerir que existen falencias importantes en el manejo y planes de contingencia para la protección de la misma al interior de las entidades estatales, puesto que en diferentes estudios como se describió anteriormente, los índices de ataques y perdidas denotan la necesidad de estrategias que contrarresten diferentes entornos para garantizar desde la capacitación hasta el encriptamiento cifrado de la misma la protección real de datos que son vitales para entidades estatales.

A pesar del diseño y desarrollo de herramientas tecnológicas, las violaciones de datos aún ocurren porque los empleados son engañados por los ataques de ingeniería social. En la mayoría de los casos de ataque, los empleados a menudo desconocen los ataques de ingeniería social y subestiman la importancia de la información aparentemente trivial para evitar un ataque exitoso, por lo tanto, es evidente la necesidad de definir un plan de acción que logre sentar las bases que sirvan para contrarrestar los ataques y a su vez permita robustecer las entidades estatales sobre cualquier ataque que se pueda llegar a presentar.

1.2 FORMULACIÓN DEL PROBLEMA

¿De qué manera el estudio sobre la ingeniería social de la información de entidades estatales impacta en la protección de la misma y sus datos fundamentales para garantizar una adecuada gestión pública?

2. JUSTIFICACIÓN

En la actualidad es conocido el crecimiento vertiginoso de la tecnología, evidenciándose a nivel mundial que las empresas están enfocadas en mantener protegido un activo importante y estratégico al interior de las mismas, el cual es la información[6], y para ello, es necesario de una gran inversión tanto en tecnología y recurso humano profesional que esté capacitado para mantener segura la información de la empresa. Muchas organizaciones formulan y anuncian políticas de seguridad. El desafío con este proceso es que los empleados generalmente ignoran o malinterpretan las políticas de la organización o intentan imaginar cómo se pueden aplicar en una situación real. Los ingenieros sociales son corruptos y utilizan diversas técnicas y canales para atacar, tales como: correo electrónico de phishing, mensajería instantánea phishing; llamada de spam, entre otras.

Debido a la importancia de la información y al crecimiento tecnológico; llama la atención que los delincuentes informáticos buscan de una manera u otra tener acceso a dicha información con un fin específico, el de afectar un sistema o exponer algún tipo de información organizacional de ámbito confidencial a través de un virus, malware, rasonware, ingeniería social, etc. En el estudio, Becker[7], argumenta que los enfoques tradicionales de obtención de requisitos se centran principalmente en el aspecto técnico de las redes, el software y los sistemas de información. Solo algunos de los enfoques en la literatura se centraron en el manejo de los ataques de ingeniería social. A medida que aumenta la cantidad de ataques de ingeniería social (SE), existe una necesidad emergente de introducir un método de obtención de requisitos de seguridad que sea divertido y fácil de realizar.

Teniendo en cuenta lo mencionado anteriormente, la ingeniería social se convierte en uno de los métodos preferidos por los delincuentes informáticos debido a que los sistemas al ser utilizados por los humanos, generan una brecha operativa; de modo que no habría sistema totalmente seguro porque la ingeniería social al involucrar al ser humano puede atacar a cualquier organización[8]. Es por esta razón, que en cada una de las entidades debe existir administradores en áreas específicas de sistemas, para que sean los encargados de salvaguardar los sistemas de información y activos informáticos importantes de la Entidad mediante protocolos de seguridad.

---

[6] GALLO, José María. La información como activo estratégico de la empresa [En línea], mayo 2014. [Consultado 18 febrero 2018]. Disponible en internet: <https://businessvalueexchange.com/es/2014/05/05/la-informacion-como-activo-estrategico-de-la-empresa/>

[7] Op Cit. Gemalto.

[8] BORGHELLO, Cristian. El arma infalible: la Ingeniería Social. San Diego California: ESET [En línea], abril 2009. p.7. Disponible en internet: <http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf>

Por consiguiente, el propósito de este estudio, es brindar una ruta mediante un Plan de Acción, el cual ayude a las Entidades Públicas de Colombia a conocer y entender que es la ingeniería social, así como la forma adecuada de contrarrestar los ataques que se pueden llegar a presentar en estas entidades.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Desarrollar un estudio basado en un análisis temático sobre la Ingeniería Social conforme a las técnicas utilizadas por los delincuentes informáticos en las Entidades Estatales, con el fin de minimizar su impacto y así evitar la pérdida de recursos financieros por fallas humanas que afecten la seguridad de la información.

3.2 OBJETIVOS ESPECÍFICOS

- Realizar un estudio del estado del arte sobre la ingeniería social, sus antecedentes, actualidad y futuro.

- Analizar la situación actual sobre ataques informáticos en las Entidades Estatales enmarcadas a nivel Gobierno.

- Definir las técnicas adecuadas para contrarrestar los ataques informáticos de Ingeniería Social de conformidad a la operación propia de las Entidades Estatales.

- Definir las etapas de un plan de acción que permita el adecuado tratamiento de las vulnerabilidades detectadas en las Entidades Estatales.

4. MARCO DE REFERENCIAL

4.1 MARCO TEORICO

4.1.1 Seguridad de la Información. Según ISO 270019, consiste en la "preservación de la confidencialidad, integridad y disponibilidad, además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad.", es decir, se busca que los sistemas que conforman la operación propia, hagan parte de la gestión global cuyo enfoque sea el tratamiento de todo tipo de riesgos que pueden poner en peligro la información de un negocio u organización, por tanto se pretende mantener y garantizar la seguridad de la misma mediante controles y estrategias adecuadas.

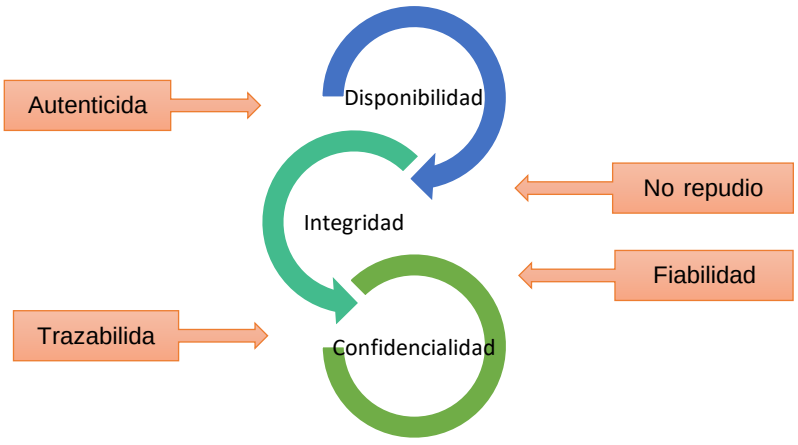
- ✓ **Confidencialidad:** "Propiedad que determina que la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados".

- ✓ **Integridad:** "Propiedad de salvaguardar la exactitud y estado completo de los activos".

- ✓ **Disponibilidad:** "Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada".

En la figura 4, se observa gráficamente las propiedades que intervienen en la seguridad de la información.

Figura 4. Propiedades de la Seguridad de la Información



Fuente: el autor, información NTC-ISO/IEC27001

[9] NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC27001-por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC)

En este contexto, se puede representar gráficamente los factores involucrados asociados con los riesgos[10], según se aprecia en la figura 5.

Figura 5. Esquema de los riesgos

Fuente: El autor, información de Mitigating the risk of social engineering attacks [En Línea]. Disponible en internet: http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1397&context=theses

Por lo anterior, se puede inferir cuando se evalúan los riesgos en la ISO 27001:2013 se refiere a las consecuencias más que a los impactos[11], puesto que los riesgos pueden afectar cualquier activo susceptible a ser dañado, robado o perdido, es por ello que debemos tener una perspectiva clara sobre los procesos de la Organización y de esta manera tener los suficientes controles determinados a través del proceso de tratamiento de los riesgos, y de esta manera se permita salvaguardar la información, a fin de proveer confianza a nivel global según las propiedades enunciadas en la figura 5.

4.1.2 Ingeniería Social. Es una forma de engañar no un sistema si no a una persona con el fin de acceder a un sistema específico o extraer información de aquella persona que tiene a su cargo información valiosa para la organización, por ende, el delincuente informático usa las fallas humanas para poder realizar el delito.

[10] ISO 27000. [En línea] Disponible en internet: <http://www.iso27000.es/sgsi.html>
[11] BSI. Group México S de RL de CV. ISO/IEC 27001 – Gestión de Seguridad de la Información – Guía de Transición.

En el año 2006 se incrementaron los ataques por medio de la técnica phishing la cual se encarga de engañar a la persona haciéndola creer que está entregando información a un sitio de confianza como el caso de Visa o MasterCard[12].

Cabe resaltar que los ataques realizados por medio de la ingeniería social no solo se realizaron utilizando como medio el sector financiero para atraer a las victimas sino también las redes sociales son utilizadas para ser suplantadas. En el estudio realizados por ESET menciona que los países Latinoamericanos más afectados por esta modalidad fueron Argentina, México y Colombia[13].

Se puede lograr a determinar algunos motivos fundamentales que llevan a hacer un ataque utilizando la ingeniería social:

- ✓ **Factor económico:** Vender la información obtenida con un fin monetario

- ✓ **Intereses personales:** El ego que lo lleva al tener acceso a información confidencial de la cual se supone que está protegida al interior de una organización.

- ✓ **Venganza:** Persona rencorosas como pueden ser ex empleados de una entidad con lo cual solo buscar causar daño al interior de la entidad.

- ✓ **Presión externa:** Puede ser causada por otros delincuentes donde se busca cual es el que más daño pueda causar o que información valiosa puede robar[14]

Los ataques de ingeniería social son mucho más sutiles y más difíciles de detectar porque involucran las actividades cotidianas que tiene una persona y se aprovecha de la confianza o seguridad que siente al hacer un proceso en específico[15].

[12] ESET Security Report Latinoamérica [En línea], 2017, [Consultado 18 febrero 2018]. Disponible en internet: <https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf>
[13] Ibíd.., p. 12.
[14] Spinapolice, Matthew. Mitigating the risk of social engineering attacks [En Línea]. Rochester Institute of Technology RIT Scholar Works, 2011. p. 3. Disponible en internet: <http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1397&context=theses>
[15] ALEXANDER, Michael. Methods for Understanding and Reducing Social Engineering Attacks [En Línea]. SANS Institute InfoSec Reading Room, 2016. p. 2 Disponible en internet: <https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972>

4.2 MARCO CONCEPTUAL

4.2.1 Ataques Remotos. Existe gran variedad de ataques a la información, los cuales influyen en la Ingeniería Social, en el caso de los ataques remotos a través de las Redes Sociales, los delincuentes buscan no solamente obtener una relación cercana con la víctima, sino también obtener información generando confianza, debido a que las personas tienden a dar a conocer toda su vida personal en estas redes.

En relación al envío de correos electrónicos el Phishing, busca sus víctimas enviando contenidos con malware o links a páginas clonadas o falsas, es decir páginas que son parecidas a las reales (Entidades Bancarias, comercio para compras con tarjetas de crédito, recolección de dineros para donaciones solidarias, entre otras.) con el fin de robar las credenciales ingresadas por las víctimas.

Otro tipo de ataque que utiliza los correos electrónicos es el Spear Phishing, donde dichos correos van dirigidos a empleados con perfiles determinados, es decir que tienen acceso a sistemas informáticos dentro de una Entidad u Organización, a fin de que sean ellos quienes suministren información interna.

Además, la técnica Telefónica, es una de las más utilizadas y efectivas, debido a que resulta cómodo para el delincuente usar un teléfono mediante una llamada para manipular las emociones de la víctima con una determinada situación, por ejemplo, un secuestro, un problema asociado a un familiar, entre otros. De manera semejante existe la técnica Vishing, donde se instauran falsos centros de atención telefónica que realizan llamadas con el propósito de efectuarse un fraude, es decir consiste en el robo de credenciales bancarias utilizando VoIP.

También existen técnicas mediante los teléfonos celulares, el Smishing (SMS), donde los delincuentes envían un mensaje de texto indicando a la víctima que ha ganado un premio, ya sea mediante un link, devolver la llamada a un número telefónico o responder un sms.

4.2.2 Ataques Locales. En lo que concierne a los ataques locales, la técnica Tailgaiting, es utilizada cuando existe una restricción de acceso físico en una Entidad (tarjeta de ingreso, etc), por tanto, el delincuente se aprovecha de la víctima a través de la buena voluntad y le indica que no trajo o se le olvido la tarjeta o dispositivo para ingresar, de esta manera manipula a la víctima para ingresar a la Entidad.

Los delincuentes también utilizan la técnica Pretexting/Impersonate, en este tipo de ataques se hacen pasar por empleados que laboran en la misma Entidad, por ejemplo, del área técnica y que le indica a la víctima que el PC que usa presenta

una anomalía que debe ser revisada, de esta manera le facilita la instalación de algún tipo de malware con el fin de tomar control del equipo para obtener información. También, los delincuentes utilizan USBs con software malicioso, mediante la técnica Baiting, buscan que la víctima realice la conexión de estos dispositivos, haciendo un estudio en el comportamiento de la persona previamente.

Sin embargo, en la técnica Shoulder Surfing, los delincuentes espían a las personas por encima del hombro, con el fin de obtener contraseñas, patrones o códigos que son utilizados en equipos o teléfonos celulares, las cuales puedan ingresar a estos dispositivos que contienen información sensible.

Aunque sea difícil de creer, los delincuentes hacen lo que sea necesario hasta el punto de registrar o revisar la basura, en la técnica Dumpster Diving, la utilizan en ocasiones cuando se arrojan documentos con información sensible (usuarios, contraseñas, entre otros) en las Entidades y que no son destruidos en su totalidad por los empleados y la cual se usa para fines fraudulentos.

4.3. MARCO LEGAL

En este proyecto se realiza una recopilación de información relacionada con los ataques informáticos en los diferentes sectores y enfocándose a nivel de gobierno donde encontramos a las Entidades Estatales; así mismo se abarcan cifras de ámbito mundial y luego se aterriza a cifras de Colombia, con el fin de tener el panorama e impacto asociado con las vulnerabilidades.

Existen organizaciones como Gemalto[16], Kaspersky[17], ESET[18], Policía Nacional de Colombia[19] que han realizado investigaciones y estudios mediante la consolidación de información, donde muestran que uno de los impactos significativos se debe a pérdidas financieras por los ataques que se presentan.

Sin embargo, a pesar de la rápida evolución en los avances tecnológicos en los últimos años y la robustez en la seguridad de los sistemas informáticos, aún existen grandes pérdidas de información que son ocasionadas por la parte humana, puesto que están expuestos a la manipulación psicológica por parte de delincuentes con el propósito de obtener un beneficio.

[16] GEMALTO. Breach Level Index. [En línea]. Disponible en internet: <http://breachlevelindex.com/>
[17] KARPERSKY LAB. Ciberamenaza Mapa Tiempo Real [En Línea]. Disponible en internet: <https://cybermap.kaspersky.com/es/stats/>
[18] ESET Security Report Latinoamérica 2017 [En línea]. ESET, 2017. [Consultado 18 febrero 2018]. Disponible en internet: <https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf>
[19] CENTRO CIBERNÉTICO POLICIAL. [En Línea], 2018. [Consultado 20 febrero 2018] Disponible en internet: <https://caivirtual.policia.gov.co/>

Conforme a la situación anterior, se crea la necesidad de aplicar normas, las cuales ayuden a proteger la información de los ciudadanos. Por esta razón en Colombia se aplican castigos jurídicos a toda persona que incurra en un delito informático. Por tanto, existe gran variedad de normatividad, la cual está enfocada a la protección de los datos personales, a la seguridad y ciberseguridad, y sirven como base jurídica para el desarrollo del estudio a realizar.

A continuación, se mencionan algunas de ellas:

Ley 527 de 1999: "Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"[20].

Ley 594 de 2000: "Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones"[21].

Ley 1266 de 2008: "Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones"[22].

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"[23].

Ley 1336 de 2009: "Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños,

[20] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527. (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial. Santafé de Bogotá, D. C., 1999. no. 43.673. 19 p.

[21] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 594. (14, julio, 2000). Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. Diario Oficial. Santa Fe de Bogotá, D. C., 2000. no.44084. 9 p.

[22] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatuaria 1266. (31, diciembre, 2018). 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.47.219. 17 p.

[23] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D. C., 2009. no. 47.223. 4 p.

niñas y adolescentes"[24].

Ley 1341 de 2009: "Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones"[25].

Ley Estatutaria 1581 de 2012: "Por la cual se dictan disposiciones generales para la protección de datos personales"[26].

Ley 1712 de 2014: "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones".

CONPES 3854: "Política Nacional de Seguridad Digital en Colombia"[27], donde el Estado se basa en principios fundamentales como; salvaguardar derechos humanos, enfoque incluyente y colaborativo, responsabilidad compartida y enfoque de gestión de riesgo.

Así mismo el Gobierno Nacional a través de la Estrategia de Gobierno en Línea se enfoca en uno de los componentes de Seguridad y privacidad de la Información y de los sistemas de información, donde cada una de las Entidades Estatales deben generar un diagnóstico de seguridad y privacidad a fin de determinar el estado actual del nivel de seguridad con el que cuentan.

Es por ello, que el Gobierno establece cinco lineamientos como marco de referencia para la elaboración de dicho diagnóstico (Entendimiento estratégico, definición de la arquitectura empresarial, análisis de riesgos, alineación del gobierno TI, proceso de gestión TI) donde los dos últimos deben alinearse con el Modelo Integrado de Planeación y Gestión, el cual se detalla en el numeral 8 del presente documento.
Según la información reportada en el Formulario Único de Reporte de Avances en la Gestión – FURAG, por todas las Entidades Estatales en la vigencia 2016 el índice

[24] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1336. (21, julio, 2009). Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Diario Oficial. Bogotá, D. C., 2009. no. 47.417. 8 p.
[25] 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. 34 p.
[26] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatutaria 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D. C., 2012. no.48587. 167p.
[27] COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1712. (06, marzo, 2014). Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Diario Oficial. Bogotá, D. C., 2014. no. 49084. 314 p.

de Gobierno en línea[28] se muestran resultados a nivel territorial (147 Entidades) con un promedio de cumplimiento del componente de seguridad y privacidad de la información del 58,5% mientras que a nivel nacional (1121 Entidades) es de un promedio del 22%. Los anteriores resultados demuestran que se debe continuar con la construcción de mecanismos que permitan a las Entidades ejercer un control, a fin de salvaguardar la información.

[28] ESTRATEGIA DE GOBIERNO EN LÍNEA. Índice de Gobierno Digital [En Línea]. Disponible en internet: <http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7651.html>

5. DISEÑO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

La metodología utilizada en el presente trabajo monográfico es descriptiva, dado que se desarrolla una investigación asociada al concepto de Ingeniería Social, ataques locales y remotos, así como métodos y técnicas utilizadas por los delincuentes informáticos para la obtención de información de sus víctimas, a fin de observar el comportamiento en el sector gobierno realizando un análisis de los datos de manera eficaz. Lo anterior, de ser necesario elevar recomendaciones mediante un plan de acción orientado a minimizar su impacto.

5.2 FUENTES Y TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

La recolección de información será dada de manera secundaria, dada a través de la observación, análisis de documentos, tesis, artículos, libros e informes asociados con la Ingeniería Social, y de esta manera especificar técnicas adecuadas conforme al conocimiento previo de la operación de las Entidades Gubernamentales y el estado actual en el que se encuentran.

5.3 POBLACIÓN Y MUESTRA

La población asociada a la monografía es propia con todas las Entidades Gubernamentales a nivel mundial teniendo en cuenta información de Europa, Estados unidos, Colombia entre otros, enmarcadas en el sector Gobierno afines con el objeto de estudio.

6. ESTUDIO DEL ESTADO DEL ARTE SOBRE LA INGENIERÍA SOCIAL, SUS ANTECEDENTES, ACTUALIDAD Y FUTURO

6.1 LA INGENIERÍA SOCIAL

El Internet está ayudando a personas de ideas afines a conectarse, comunicarse, compartir y difundir su punto de vista, sin embargo, en esta era digital en la que conectarse con las personas no es un problema, los atacantes también tienen acceso a un público más amplio mientras permanecen en el anonimato. Los ingenieros sociales, los extremistas y otros actores negativos de la sociedad están usando internet para difundir propaganda, conspiraciones e ideologías. Pese a que existe el diseño y desarrollo de herramientas tecnológicas, las violaciones de datos aún ocurren porque los empleados son engañados por los ataques de ingeniería social. En la mayoría de los casos de ataque, los empleados a menudo desconocen los ataques de ingeniería y subestiman la importancia de la información aparentemente trivial para evitar un ataque exitoso. Muchas organizaciones formulan y anuncian políticas de seguridad. El desafío con este proceso es que los empleados generalmente ignoran o malinterpretan las políticas de la organización o intentan imaginar cómo se pueden aplicar en una situación real. Los ingenieros sociales son corruptos y utilizan diversas técnicas y canales para atacar, tales como: correo electrónico de phishing; llamada de spam, entre otros.[29]

Como base para el estudio monográfico se realiza la consulta de diferentes fuentes como lo son universidades, entidades y organizaciones, etc. donde se fundamenta una investigación y análisis sobre la ingeniería social la cual ayudara a fundamentar el desarrollo del estudio monográfico.

6.2 ANTECEDENTES

Los seres humanos que son usuarios, se consideran el eslabón más débil en el dominio de seguridad de la información, una de las posibles razones es que los humanos confían entre sí y comparten información personal con bastante rapidez, esto se evidencia ante la existencia de varios estudios de investigación intentaron proponer soluciones únicas que pueden ser efectivas para proteger los ataques de ingeniería social o útiles para mitigar el peligro: entre los que se destacan cuya investigación tiene como objetivo verificar si el cebado mediante señales y advertencias es efectivo para contrarrestar el hábito de revelar información personal información. Se realizó un experimento en un centro comercial en Holanda, el estudio demostró que pese a las advertencias, los visitantes compartieron sus

[29] SABOUNI S, CULLEN A, ARMITAGE L. Un marco preliminar de radicalización basado en técnicas de ingeniería social. Conferencia internacional de 2017 sobre conciencia cibernética situacional, análisis y evaluación de datos (Cyber SA). Londres, Reino Unido: IEEE. 2017

identificaciones de correo electrónico, 9 de los 18 dígitos de su número de cuenta bancaria y otra información personal. El análisis mostró además que el 79.1% de los participantes compartieron sus direcciones de correo electrónico y el 43.5% proporcionó la información de su cuenta bancaria.[30] (Heartfield, Loukas, 2018).

Para los compradores en línea, el 89.8% de ellos entregó información con respecto a su compra y el 91.4% compartió el nombre de la tienda en línea desde donde suelen comprar. Además, el análisis multivariado mostró que el cebado y las advertencias por sí solas no son efectivos para mitigar la tendencia humana a revelar información en línea. [31]

De igual forma, otro estudio, SCHAAB[32] al propuso un concepto de que los humanos pueden usarse como un sensor de seguridad. La idea básica era crear una aplicación prototipo que se instalará en la plataforma de Windows del participante. Tan pronto como el participante detecte cualquier spam o ataque semántico, él o ella presentarán los detalles en la aplicación prototipo. Por lo tanto, si participan más y más usuarios, es menos probable que un ataque de ingeniería social tenga éxito. Este concepto, en otros términos, se conoce como crowdsourcing, donde la multitud es la principal fuente de información, datos, etc. Este "estudio" esencialmente, propuso la arquitectura del software humano como marco de sensores de seguridad e implementó y evaluó empíricamente la efectividad de herramienta desarrollada.

Otras investigaciones realizadas por Edwards et al[33], verificaron la herramienta creada para extraer información en línea y afirmaron además que el analizador automático de escáner propuesto podría usarse para verificar la vulnerabilidad de una organización; de igual forma trataron de identificar los factores humanos vulnerables y sus posibles relaciones con los ataques de ingeniería social y los requisitos de seguridad.

Las amenazas que se han dirigido principalmente a las entidades públicas y diferentes organismos gubernamentales, han expandido la zona objetivo para incluir los sectores privado y corporativo. Esta clase de amenazas, bien conocidas como Amenazas Persistentes Avanzadas (APT), son aquellas contra las cuales toda nación y organización bien establecida teme y quiere protegerse. Si bien los ataques

[30] HEARTFIELD R, LOUKAS G. Detectando ataques semánticos de ingeniería social con el eslabón más débil: implementación y evaluación empírica de un marco humano como sensor de seguridad. 2018. En línea. Recuperado de: http://www.sciencedirect.com/science/article

[31] JUNGER M, MONTOYA L, OVERINK FJ El cebado y las advertencias no son efectivos para prevenir ataques de ingeniería social. Comput Hum Behav. 2017. En línea. Recuperado de: https://doi.org/10.1016/j.chb.2016.09.012

[32] SCHAAB P, BECKERS K, PAPE S. Mecanismos de defensa de ingeniería social y estrategias de formación contrarias. Inf Comput Secur. 2017. En línea. Recuperado de: https://doi.org/10.1108/ICS-04-2017-0022

[33] EDWARDS M, LARSON R, GREEN B, RASHID A, BARON A. (2017). Búsqueda de oro: análisis automático de superficies de ataque de ingeniería social en línea. Comput Secur. 2017.

APT patrocinados por entes públicos, como ministerio de defensa en contra de páginas de pornografía infantil para citar un ejemplo, siempre estarán marcados por su sofisticación, los APTattacks que se han vuelto prominentes en los sectores corporativos no lo hacen menos desafiante para las organizaciones[34].

La velocidad a la que evolucionan las herramientas y técnicas de ataque está haciendo que cualquier medida de seguridad existente sea inadecuada. A medida que los defensores se esfuerzan por asegurar cada punto final y cada enlace dentro de sus redes, los atacantes están encontrando nuevas formas de penetrar en sus sistemas objetivos. Con cada día trayendo nuevas formas de malware, con nuevas firmas y un comportamiento cercano a lo normal, un solo sistema de detección de amenazas no sería suficiente. Si bien requiere tiempo y paciencia para realizar APT, se requieren soluciones que se adapten al comportamiento cambiante de los atacantes APT[35].

Se han publicado varios trabajos sobre la detección de un ataque APT en una o dos de sus etapas, pero existe una investigación muy limitada en la detección de APT en su conjunto desde el reconocimiento hasta la limpieza, ya que esta solución exige una correlación compleja y un análisis de comportamiento fino de usuarios y sistemas dentro y a través de redes.

Debido al fuerte énfasis en la seguridad de la información por parte de los investigadores de seguridad en todo el mundo, la seguridad que alguna vez fue exclusiva de las organizaciones militares y bien establecidas ahora ha comenzado a formar parte de cada organización. Sin embargo, esto no es suficiente ya que cada día se nos presenta un nuevo tipo de malware y una nueva forma de ataque.

6.3 ACTUALIDAD

Los ataques de ingeniería social generalmente explotan la psicología humana y la susceptibilidad a la manipulación para engañar a las víctimas para que descubran datos confidenciales o rompan las medidas de seguridad que permitirán que un atacante acceda a la red. Algo que hace que los ataques de ingeniería social sean uno de los tipos más peligrosos de amenazas de red es la falta general de cultura de ciberseguridad. En una organización, los empleados son la primera línea de defensa, y con demasiada frecuencia son el eslabón más débil, tanto que todo lo que se necesita es que un empleado haga clic en un vínculo sospechoso para costarle a la empresa decenas de miles de dólares.

---

[34] X. Wang, K. Zheng, X. Niu, B. Wu y C. Wu, "Detección de comando y control en amenazas persistentes avanzadas basadas en acceso independiente", en Comunicaciones (ICC), Conferencia Internacional IEEE 2016 en IEEE, 2016

[35] M. Marchetti, F. Pierazzi, A. Guido y M. Colajanni, “Contrarrestar las amenazas persistentes avanzadas a través de la inteligencia de seguridad y análisis de datos grandes”, en Cyber Con fl ict (CyCon), 2016 8ª Conferencia Internacional sobre. IEEE, 2016

Los sistemas de comunicación son vulnerables y pueden ser fácilmente penetrados por usuarios maliciosos a través de ataques de ingeniería social. Estos ataques tienen como objetivo engañar a las personas o empresas para que realicen acciones que beneficien a los atacantes o les proporcionen datos confidenciales como el número de seguro social, los registros de salud y las contraseñas. La ingeniería social es uno de los mayores desafíos que enfrenta la seguridad de la red porque explota la tendencia humana natural a confiar.

Con la aparición de Big Data, los atacantes usan esta información para capitalizar datos valiosos para fines comerciales. Empaquetan grandes cantidades de datos para venderlos a granel como bienes de los mercados actuales.

Aunque los ataques de ingeniería social difieren entre sí, tienen un patrón común con fases similares. El patrón común implica cuatro fases: recopilar información sobre el objetivo; desarrollar una relación con el objetivo; explotar la información disponible y ejecutar el ataque; y salir sin dejar rastros.[36]

Los ataques de base técnica se llevan a cabo a través de Internet a través de redes sociales y sitios web de servicios en línea y recopilan la información deseada, como contraseñas, detalles de tarjetas de crédito y preguntas de seguridad. Los ataques físicos se refieren a acciones físicas realizadas por el atacante para recopilar información sobre el objetivo. Un ejemplo de tales ataques es la búsqueda en contenedores de documentos valiosos.[37] Los ataques de ingeniería social pueden combinar los diferentes aspectos discutidos previamente, a saber: humanos, informáticos, técnicos, sociales y físicos. Los ejemplos de ataques de ingeniería social incluyen suplantación de identidad, suplantación de llamadas a la mesa de ayuda, navegación de hombros, buceo en basurero, robo de documentos importantes, robo de desvío, software falso, cebo, quid pro quo, pretexting, tailgating, ventanas emergentes, llamadas automáticas, ransomware, en línea ingeniería social, ingeniería social inversa e ingeniería social telefónica. [38]

[36] Pokrovskaia, N. Ingeniería social y tecnologías digitales para la seguridad del desarrollo del capital social. En Actas de la Conferencia Internacional de Gestión de Calidad, Transporte y Seguridad de la Información, Petersburgo, Rusia, 24-30 de septiembre de 2017; pp. 16

[37] Costantino, G .; La Marra, A .; Martinelli, F .; Matteucci, I. CANDY: Un ataque de ingeniería social para filtrar información del sistema de infoentretenimiento. En Actas de la Conferencia de Tecnología Vehicular IEEE, Oporto, Portugal, del 3 al 6 de junio de 2018; pp. 1-5

[38] Mahmood, U .; Afzal, T. Análisis de seguridad: análisis de Big Data para ciberseguridad: una revisión de tendencias, técnicas y herramientas. En Actas de la Conferencia Nacional de IEEE sobre Aseguramiento de la Información, Rawalpindi, Pakistán, 11-12 de diciembre de 2013; pp. 129-134

6.4 FUTURO

Se requiere acciones políticas para que todas las partes interesadas en Colombia puedan llevar a cabo sus actividades socioeconómicas en ese entorno de manera segura y confiable.

Colombia, con una población estimada de 49.5 millones en 2017, tenía 62.7 millones de suscriptores móviles para el mismo año, según el Ministerio de Tecnología de la Información y Comunicaciones (MINTIC). Hubo 14,6 suscripciones a líneas fijas por cada 100 habitantes en 2016. MINTIC también informó 16,6 millones de suscripciones a Internet en 2017, lo que representa una tasa de penetración del 33,7%.[39]

Según un estudio encargado por el Ministerio de TIC, Facebook (88%), WhatsApp (87%), YouTube (51,6%), Instagram (34%), Google Plus (29%), Twitter (20%) y Snapchat (7,2%) son las redes sociales más utilizadas.

El marco legal colombiano proporciona una serie de protecciones esenciales para el derecho a la privacidad, tanto en el texto de la Constitución de 1991 como en el instrumento constitucional (bloque de constitucionalidad) de conformidad con el artículo 92 de la Constitución colombiana. Este artículo incorpora las obligaciones internacionales de derechos humanos de Colombia en la legislación colombiana y les confiere el estado de derecho constitucional, lo que significa que tienen prioridad sobre las disposiciones legales.

El Informe de Riesgo Global 2019 (WEF, 2019) presenta los resultados de la Encuesta de percepción de riesgo global que involucra a alrededor de 1,000[40] tomadores de decisiones del sector público, el sector privado, la academia y la sociedad civil que evalúan los riesgos generales que enfrenta el mundo. En este sentido, aproximadamente dos tercios de los encuestados esperan que los riesgos asociados con las noticias falsas y el robo de identidad aumenten en 2019, mientras que tres quintos dicen lo mismo sobre la pérdida de privacidad para las organizaciones y los gobiernos. Además, señala entre los diez riesgos principales en términos de probabilidad de ocurrencia, el de "," Fraude o robo de datos "en la posición cuatro y" ataques cibernéticos "en la posición cinco, mientras que, en términos de impacto, apunta a" ataques cibernéticos "en la posición siete e"

[39] Sophos 2020 Threat Report. In an experiment, Sophos set up honeypot machines in data centers located around the world. Some received nearly 600,000 brute-force login attempts. https://www.sophos.com/en-us/medialibrary/pdfs/technical-papers/sophoslabs-uncut-2020-threat-report.pdf

[40] CONPES 10.24. En línea. Recuperado de: https://webcache.googleusercontent.com/search?q=cache:sHf7Q4ul6j0J:https://www.dnp.gov.co/CONPES/Documents/2019-10-24%2520Documento%2520CONPES%2520National%2520Policy%2520for%2520Digital%2520Trust%2520and%2520Security.pdf+&cd=1&hl=es-419&ct=clnk&gl=co#20

infraestructura crítica " fracaso "en la posición ocho. Estos riesgos asociados con el uso de la tecnología superan a otros como" desastres ambientales provocados por el hombre "e incluso" propagación de enfermedades infecciosas "en la evaluación, lo que destaca el nivel de importancia de los aspectos de seguridad digital y debería motivar a los Estados a tome mayores medidas para abordar estos riesgos.

6.5 ESTADO DEL ARTE

Un escrito realizado por Monsalve[41] su principal objetivo fue presentar la actualidad de las amenazas y ciberataques al que se compromete el recurso humano en la red de cualquier empresa en Colombia. Se trataron las amenazas más estudiadas y como estas se pueden beneficiar hoy en día del recurso humano, el cual es la pieza más débil de cualquier empresa ya sea grande, mediana o pequeña y de su respectiva información. La tecnología y la información hacen continuamente el mundo esté conectado y se pueda compartir información sensible tal como información bancaria, historial clínico, datos personales etc. El valor comercial de la información no tiene precedente para los ciberdelincuentes (personas con conocimiento suficiente para vulnerar cualquier sistema de información) y es vendida en un mercado por un valor infravalorado a personas con pretensiones de extorsionar o perpetuar ciberataques con fines lucrativos.

Un documento titulado Vulnerabilidad a la Ingeniería Social en Social Redes: un marco propuesto centrado en el usuario, escrito por Samar Albladi and George R S Weir[42], en este artículo se hace énfasis en los sitios de redes sociales, los cuales poseen millones de usuarios que se comunican y comparten su información personal todos los días, así como comparten estados que le permiten a otros conocer sus movimientos y actividades. Es así, que describen la ingeniería social como una de las mayores amenazas para la seguridad de la información actualmente. La ingeniería social es una técnica de ataque para manipular y engañar a los usuarios a fin de acceder u obtener información privilegiada, y acceden a través de estrategias que los usuarios no desconfían y acceden a brindar datos importantes que son usados para destinos fraudulentos.

Sin embargo, el número de ataques de ingeniería social ha aumentado dramáticamente en los últimos años, causando daños desagradables tanto a organizaciones como a individuos, pero pese a ello existe poca investigación que

[41] MONSALVE, JAIME. CIBERSEGURIDAD: PRINCIPALES AMENAZAS EN COLOMBIA (INGENIERÍA SOCIAL, PHISHING Y DoS). Artículo. En línea. Recuperado de: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4663/00004883.pdf?sequence=1&isAllowed=y

[42] Samar A y George R. Vulnerabilidad a la Ingeniería Social en Social Redes: un marco propuesto centrado en el usuario. Artículo. Traducción. En línea. Recuperado de: https://pure.strath.ac.uk/ws/portalfiles/portal/63205006/Albladi_Weir_ICCCF2016_Vulnerability_to_social_engineering_in_social_networks.pdf

ha discutido la ingeniería social en los entornos virtuales de las redes sociales. Pues se carece de sustento para contrarrestar estos exploits para comprender por qué las personas son víctimas de tales ataques. A partir de ello no existe investigación sobre ingeniería social y el engaño, esto no ha logrado identificar satisfactoriamente los factores que influyen en la capacidad de los usuarios para detectar ataques.

Otra investigación titulada ¿Podemos combatir los ataques de ingeniería social por medios sociales? Evaluar la prominencia social como un medio para mejorar la detección de phishing, escrita por Nicholson[43], los autores hacen alusión al tipo de ataque más conocido el cual es el phishing, que es una forma muy frecuente de ingeniería social en la que un atacante roba información confidencial mediante el envío de correos electrónicos fraudulentos que pretenden ser de una fuente confiable. Con el tiempo, los ataques de phishing se han vuelto más inteligentes social y contextualmente, con el resultado de que el phishing sigue siendo un problema creciente para organizaciones e individuos. En el mejor de los casos, los resultados de phishing en la pérdida de productividad debido a que los usuarios deliberan sobre la autenticidad del correo electrónico, pero en el peor de los casos, las personas y las empresas pueden sufrir serias pérdidas de seguridad, financieras y / o de reputación debido a credenciales robadas o información filtrada.

Es por ello, que no existen probabilidades medibles que permitan determinar que los usuarios tomen medidas efectivas contra los ataques de phishing a menos que sean conscientes de los riesgos inherentes a la comunicación en línea y también conozcan las amenazas específicas que representan los correos electrónicos dudosos, es por ello que la ingeniería social se ha vuelto uno de los delitos más significativos asociado a las nuevas tecnologías informáticas y que actualmente no posee filtros suficientes para contrarrestarla.

Además, el conocimiento de ciberseguridad de los usuarios (es decir, phishing) está relacionado positivamente con su actitud e intención hacia la adopción y el uso de soluciones de ciberseguridad (anti-phishing). No es sorprendente, entonces, que se hayan desarrollado una serie de intervenciones educativas diseñadas para mejorar la comprensión del usuario sobre el riesgo y el conocimiento de cómo mitigar el riesgo. Estas intervenciones adoptan una amplia gama de diferentes técnicas de entrenamiento que pueden incluir sistemas de entrenamiento integrados dibujos animados motivacionales e incluso juegos que crean conciencia y capacitan a los usuarios para futuros encuentros[44].

[43] Nicholson J; Coventry L y Briggs R. ¿Podemos combatir los ataques de ingeniería social por medios sociales? Evaluar la prominencia social como un medio para mejorar la detección de phishing,

[44] Ferreira, A., Coventry, L. y Lenzini, G. Principios de persuasión en ingeniería social y su uso en phishing. Lecture Notes in Computer Science (incluidas las subseries Lecture Notes in Artificial Intelligence y Lecture Notes in Bioinformatics) (2015)

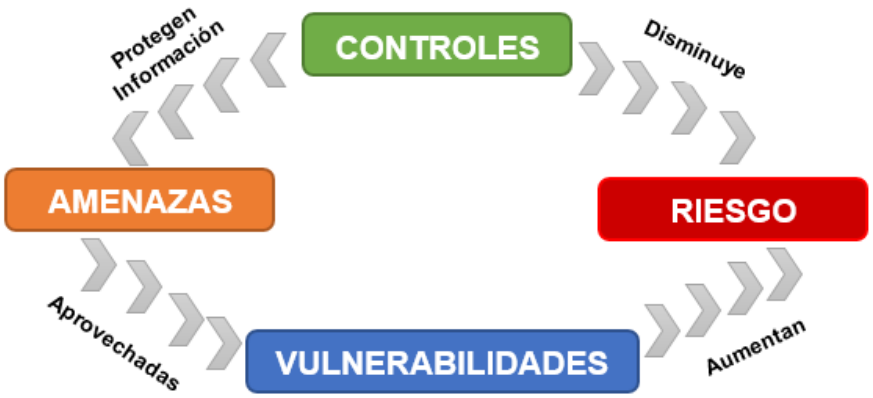
A través de los últimos tiempos, la historia del concepto de ingeniería social en ciberseguridad y argumenta que, si bien el término comenzó su vida en el estudio de la política, y solo más tarde se usó en el dominio de la ciberseguridad, estas son aplicaciones de las mismas ideas fundamentales: simetría epistémica, dominio tecnocrático y el reemplazo teleológico.[45]

[45] Larissa Zakharova, "La communication totalitaire, une technique d'ingénierie sociale", Books and Ideas, 23 mars 2011. ISSN: 2105-3030. http://www.laviedesidees.fr/La-communication-totalitaire-une.html

7. TIPOS DE ATAQUES

En relación a la Seguridad de la Información, existe infinidad de amenazas que son aprovechadas por las vulnerabilidades y que aumentan los riesgos, por tanto, es necesario que sean disminuidos con adecuados controles, los cuales protegen la información de dichas amenazas (Ver flujo en la figura 6).

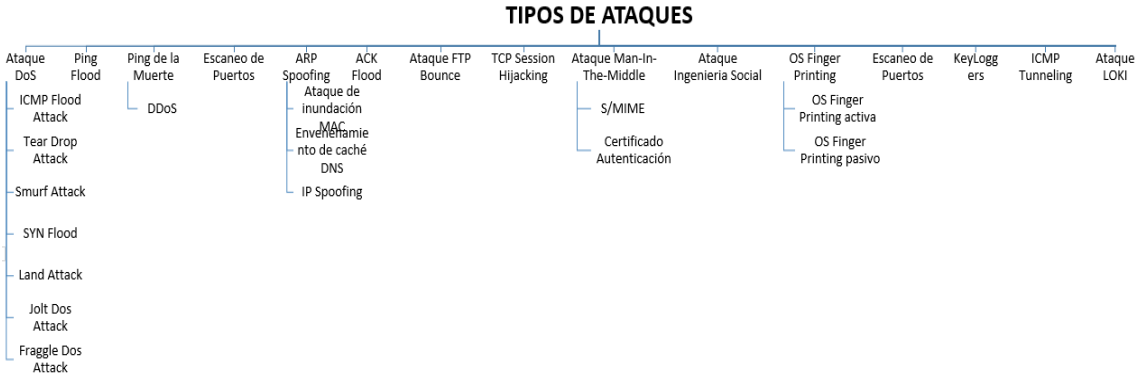
Figura 6. Interacción de los riesgos



Fuente: El autor

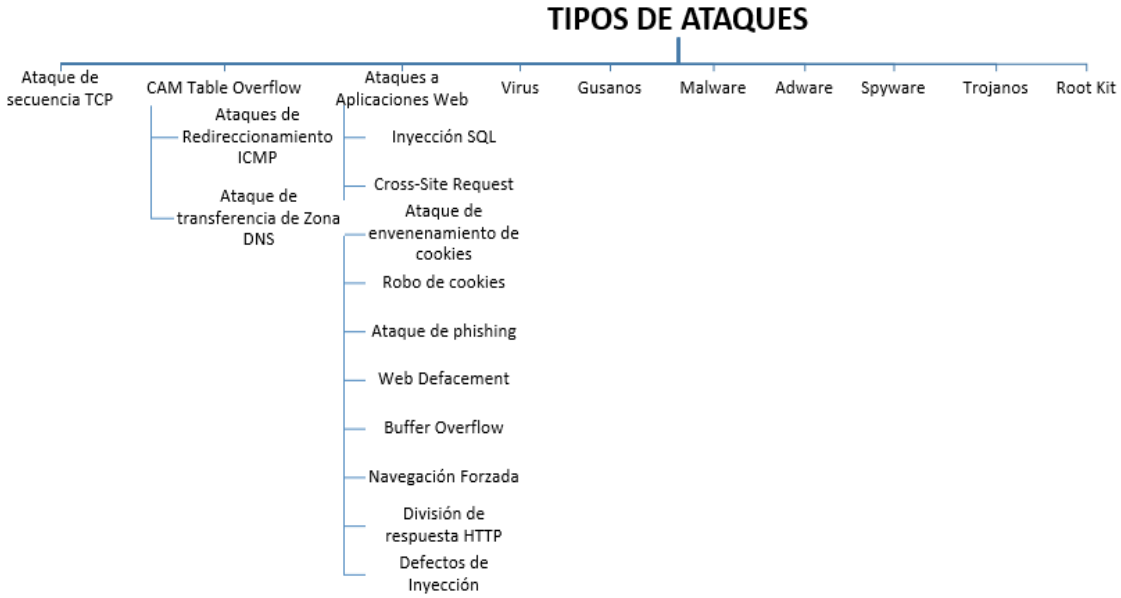
En dicho contexto y teniendo en cuenta las amenazas que se pueden presentar en cualquier organización o relacionado al ámbito personal, es absurdo definir una lista concreta con todos los tipos de ataques, según Ramiro Rubén, define 25 de ellos[46], como se observa en la figura 7.

Figura 7. Esquema Tipos de Ataques



[46]RUBÉN, Ramiro. 25 Tipos de ataques informáticos y cómo prevenirlos [En Línea]. Ciberseguridad 2018. Disponible en internet: <https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/>

Figura 7. (Continuación)



Fuente: El autor.

Dentro de estos ataques se encuentra la Ingeniería Social, la cual se basa en la manipulación psicológica, es decir, lograr que las personas sean quienes suministren la información requerida para el delincuente pueda efectuar el delito mediante engaños.

En el numeral 4.2, se detallaron cada uno de los ataques tanto remotos como locales. En la vigencia 2015 se revelo en un informe de la Industria que la Ingeniería Social se enfoca en las Empresas, donde los delincuentes usan este tipo de ataque en los mandos medios y altos ejecutivos para llevar a cabo el delito[47], según Richard De Vere, consultor de Ingeniería Social y pentester en The AntiSocial Engineer Limited, indico que son una “mina de oro” [48].

[47] WeLiveSecurity. Editor de ESET.com. 5 Cosas que debes saber sobre la Ingeniería Social. - Noticias, opiniones y análisis de la comunidad de seguridad de ESET. [En Línea]. 2016. Disponible en internet https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/

[48] DE VERE, Richard. Rubbish Security. [En Línea], 2015. [Citado 20 febrero 2018]. Disponible en <https://theantisocialengineer.com/2015/11/07/rubbish-security/>

8. SITUACION ACTUAL ATAQUES

De conformidad a Kaspersky Lab, se presentan una serie de estadísticas de las ciberamenaza en tiempo real. A nivel de Colombia desde el 13 de febrero al 12 de marzo de 2018 en lo que respecta Amenazas Web, existen dos incrementos en los días, 20 de febrero con 81253 amenazas y el 07 de marzo con 71809 amenazas. Así mismo Kaspersky muestra que el 90.68% se debe al Trojan.Script.Generic[49].

Muchos ataques están camuflados a través del Pretexting, que es otra forma de ingeniería social donde los atacantes se centran en crear un buen pretexto, o un escenario inventado, que usan para tratar de robar la información personal de sus víctimas. En este tipo de ataques, el estafador generalmente dice que necesitan ciertos bits de información de su objetivo para confirmar su identidad. En realidad, roban esos datos y los usan para cometer robo de identidad o realizar ataques secundarios.

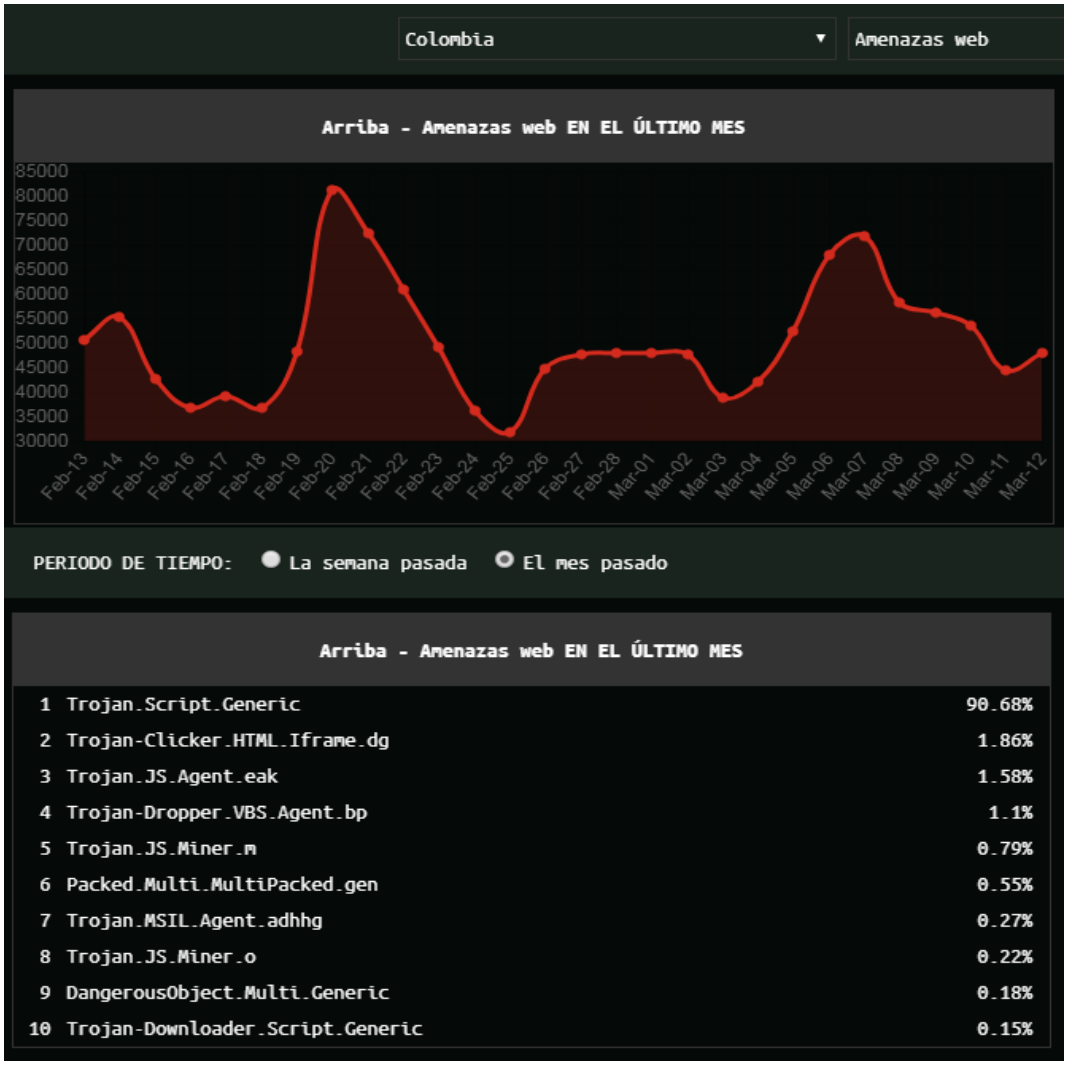
Los ataques más avanzados a veces intentan engañar a sus objetivos para que hagan algo que abusa de las debilidades físicas y digitales de una organización. Por ejemplo, un atacante podría hacerse pasar por un auditor externo de servicios de TI para que pueda convencer al equipo de seguridad física de una empresa objetivo de que lo deje entrar al edificio.

Mientras que los ataques de phishing utilizan principalmente el miedo y la urgencia para su ventaja, los ataques de pretexto dependen de construir un falso sentido de confianza con la víctima. Esto requiere que el atacante construya una historia creíble que deje poco espacio para la duda por parte de su objetivo.

Actualmente Colombia no escapa de estos tipos de fenómenos como se muestra en la figura 8.

[49] Kaspersky Lab. Ciberamenaza Mapa Tiempo Real [En Línea]. Disponible en internet: <https://cybermap.kaspersky.com/es/stats/>

Figura 8. Situación Actual – Amenazas Web Colombia

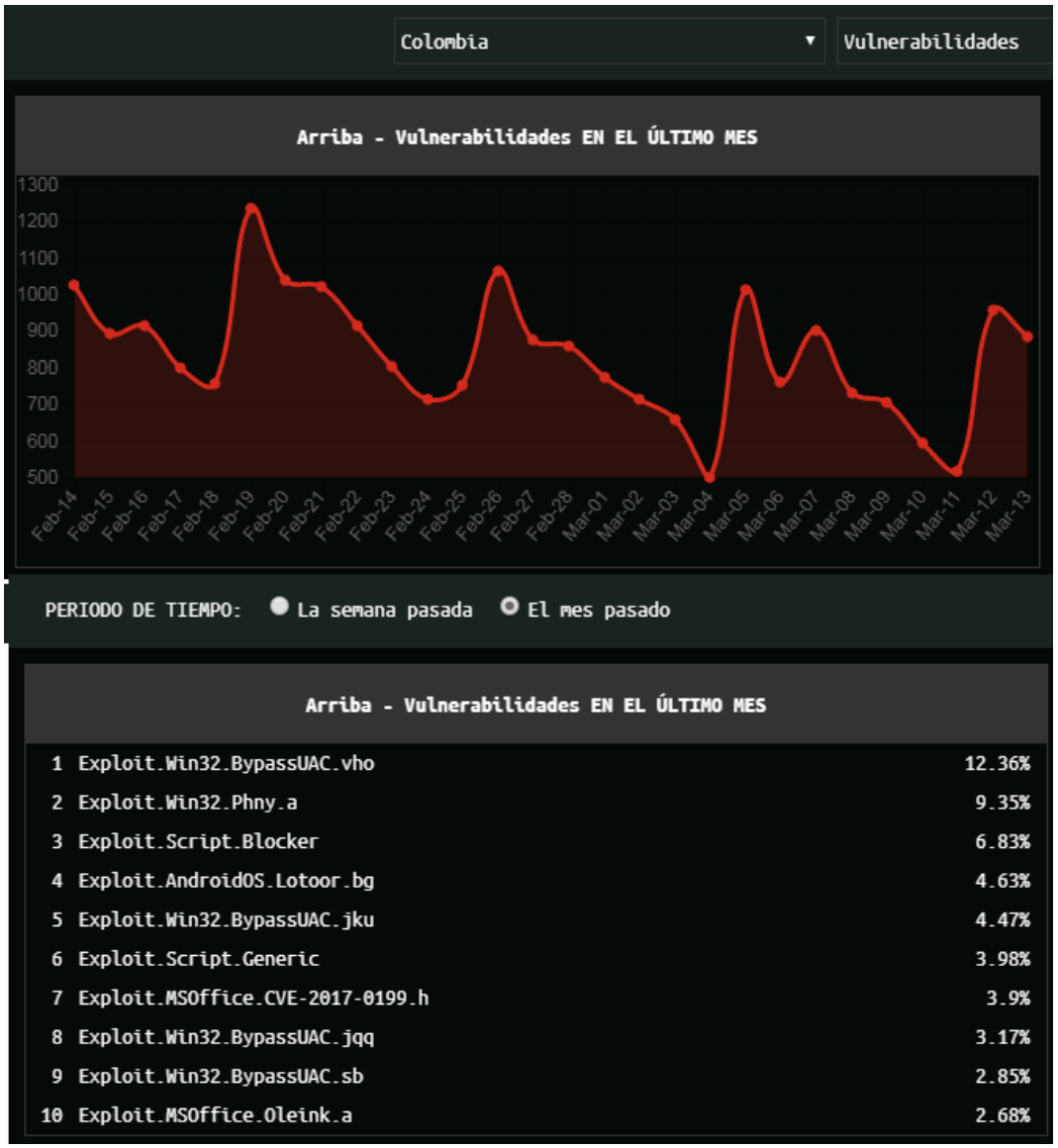


Fuente: Kaspersky Lab. Ciberamenaza Mapa Tiempo Real [En Línea]. Disponible en internet: https://cybermap.kaspersky.com/es/stats/

Así mismo se detalla en el Lab de esta empresa Rusa Kaspersky, que las vulnerabilidades en Colombia han tenido un comportamiento oscilador desde el 14 de febrero al 13 de marzo de 2018, como se aprecia en la figura 9; siendo de mayor porcentaje con el 12.36% Exploit.Win32.BypassUAC.vho[50].

[50] Ibid.

Figura 9. Situación Actual - Vulnerabilidades Colombia

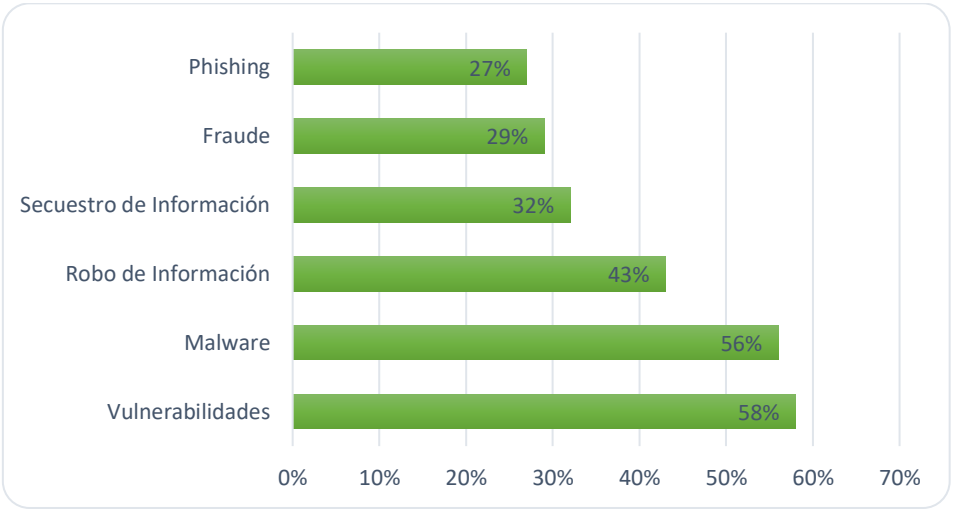


Fuente: Kaspersky Lab. Ciberamenaza Mapa Tiempo Real [En Línea]. Disponible en internet: https://cybermap.kaspersky.com/es/stats/

Por otra parte, una de las empresas con más de 20 años de experiencia en proveer estrategias en seguridad de la Información en Latinoamérica, es Digiware. Esta compañía público en la vigencia 2017 que el Cibercrimen en Colombia presento las cifras; el 46.7% de las empresas sufrieron algún incidente informático, el 16% fue

víctima de ransomware, el 49% sufrió una infección de malware, el 15% fue víctima de phishing, el 10 % fue víctima de exploits y el 9 % sufrió ataques de DoS[51].
De igual manera Digiware informa que las Empresas presentan mayor preocupación a las vulnerabilidades con el 58% según se observa en la figura 10.

Figura 10. Preocupaciones de las Empresas



Fuente: Digiware. Cibercrimen en Colombia. [En Línea]. Disponible en internet: http://www.digiware.net/sites/default/files/doc_digiware_infografias/Infografia-Cibercrimen-en-Colombia.png

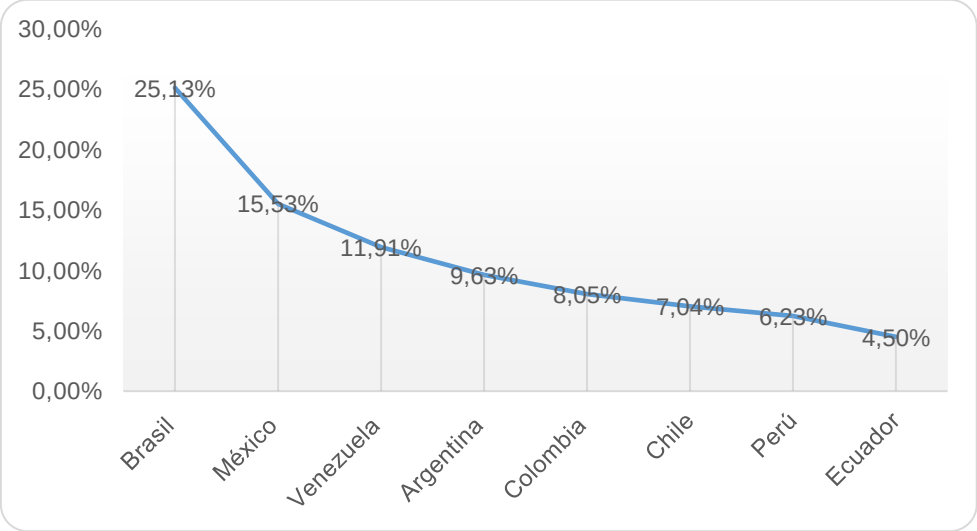
Según Andrés Galindo experto en Ciberseguridad de Digiware indico que “Lo más común es intentar atacar al usuario. En las empresas hay diferentes tipos de controles, pero si logras ‘hackear’ al usuario (a través de engaños en correos, por ejemplo), todos esos millones de inversión en seguridad informática se pierden” [52]. Por lo anterior se puede inferir que se debe prestar mayor atención al usuario y no solo realizar grandes inversiones en los Sistemas de Información de las Empresas, ya que las personas son el comodín que utiliza el delincuente para aprovechar estas vulnerabilidades y de esta manera cometer el delito fácilmente.

A nivel de América Latina las cifras son alarmantes, en el 2017 Digiware informo los sectores económicos y países afectados por el Cibercrimen. El país más afectado

[51] Digiware. Cibercrimen en Colombia. [En Línea], septiembre 2017. Disponible en internet: <http://www.digiware.net/sites/default/files/doc_digiware_infografias/Infografia-Cibercrimen-en-Colombia.png>
[52] TECNÓSFERA – El Tiempo. A diario se registran 542.465 ataques informáticos en Colombia. [En Línea], septiembre 2017. [Citado en 22 de febrero de 2018]. Disponible en internet: <https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-135370>

es Brasil con el 25,13% mientras que Colombia se encuentra en el quinto lugar con el 8.05% como se puede observar en la figura 11[53].

Figura 11. Países afectados por delitos informáticos de América Latina



Fuente: Digiware. [En Línea]. Disponible en internet: http://www.digiware.net/

En base a las diversas modalidades de ataques, las pérdidas para Colombia se reflejaron con US$ 6.179 millones como se puede evidenciar en la Tabla 1, de igual manera se muestran las perdidas en Chile, Perú y Ecuador.

Tabla 1. Perdidas en Millones de Dólares en América Latina

	% Delitos Informáticos	Perdidas (millones de dólares)
Colombia	8,05%	6,179
Chile	7,04%	5,404
Perú	6,23%	4,782
Ecuador	4,50%	3,456

Fuente: Digiware. [En Línea]. Disponible en internet: http://www.digiware.net/

En promedio en Colombia se generan 542.465 ataques informáticos y a nivel de Gobierno ocupa el tercer puesto con el 15.44% con 83.756 ataques por día. A continuación, se representa en la Tabla 2 la distribución de los ataques por sectores económicos.

[53] Digiware. [En Línea]. Disponible en internet: http://www.digiware.net/

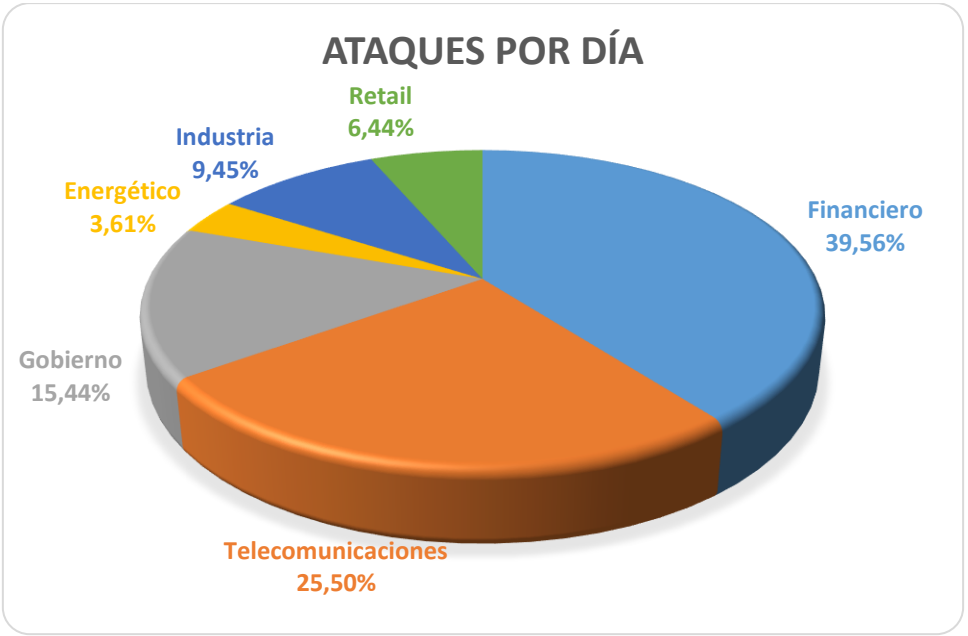
Tabla 2. Ataques por día por Sector Económico

SECTOR	ATAQUES POR DÍA
Financiero	214.600
Telecomunicaciones	138.329
Gobierno	83.756
Energético	19.583
Industria	51.263
Retail	34.934

Fuente: Digiware. [En Línea]. Disponible en internet: http://www.digiware.net/

Así mismo se presenta gráficamente el porcentaje por sector económico como se puede evidenciar en la figura 12.

Figura 12. Porcentaje por sector económico de Ataques en Colombia



Fuente: Digiware. [En Línea]. Disponible en internet: http://www.digiware.net/

Aunado con lo anterior y la percepción y resultados obtenidos por los expertos; así mismo Computerworld Colombia, en una de sus publicaciones manifiesta que los ataques de seguridad continuaran siendo protagonistas en la vigencia 2018, puesto

que “ninguna seguridad es completa si las personas no tienen la cultura de seguridad”[54].

La Policía Nacional de Colombia a través del Centro Cibernético Policial y su observatorio de Cibercrimen ofrece un espacio en atención en línea policial, siendo una iniciativa en Iberoamérica sobre la socialización de temas asociados con la ciberseguridad, Cibercrimen, entre otros[55].

Para la vigencia 2017 la Policía a través de este observatorio identifico nuevas modalidades delictivas[56]. Según la tabla 3 se muestran aquellas, que generaron pérdidas millonarias.

Tabla 3. Casos reportados y pérdidas generadas

	Casos Reportados	**Perdidas (Miles de Millones)**
a) Estafa por suplantación de Sim Card	1.385	7.690
b) Vishing	1.055	2.132
c) Ciberpirámides	182	1.500

Fuente: Centro Cibernético Policial. Informe Balance Cibercrimen en Colombia 2017. [En Línea]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

a) Estafa por suplantación de Sim Card: Mediante la suplantación, el criminal obtiene una nueva sim con el Operador del titular donde tiene la línea móvil, con el propósito de sincronizar redes sociales y productos financieros para realizar delitos.

b) Vishing – Tráfico de datos financieros personales: En esta modalidad delictiva los delincuentes aplican Ingeniería Social telefónicamente.

c) Ciberpirámides: Son recaudos de dineros mediante la estafa masiva, donde los delincuentes llaman la atención de inversionistas para supuestas compras en monedas Bitcoin, Ripple o Etherreum.

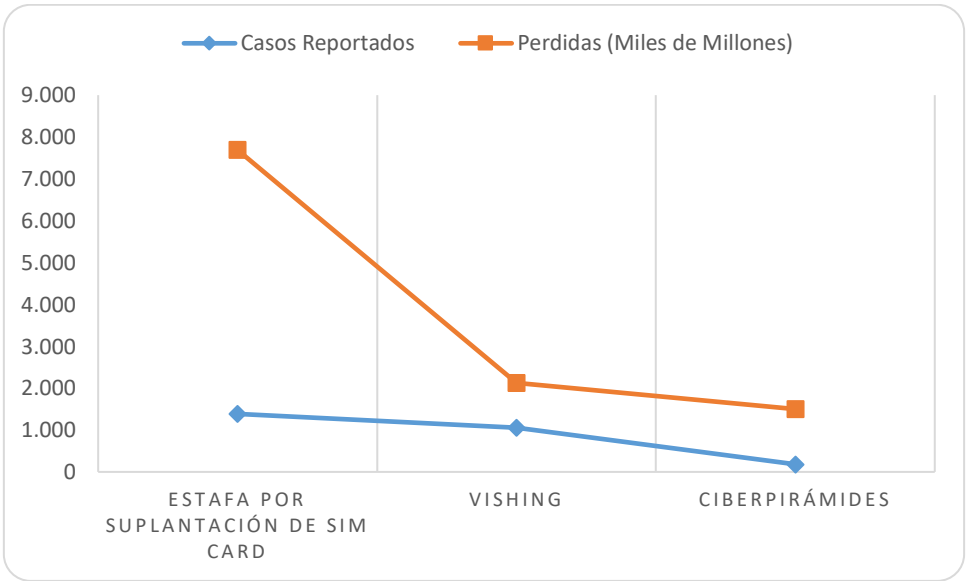
[54] Computerworld Colombia. Ataques en seguridad seguirán siendo protagonistas en 2018. [En Línea]. Disponible en: https://computerworld.co/ataques-en-seguridad-seguiran-siendo-protagonistas-en-2018/
[55] Centro Cibernético Policial. [En Línea]. Disponible en: https://caivirtual.policia.gov.co/
[56] Centro Cibernético Policial. Informe Balance Cibercrimen en Colombia 2017. [En Línea]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

d) Ciberinducción a daños físicos, mediante las redes sociales los niños, niñas y adolescentes establecían retos para autolesionarse.

e) Fraude por falso WhatsApp: Los delincuentes utilizan aplicaciones alojadas en tiendas virtuales, con el fin de crear falsas conversaciones que son enviadas por medio de pantallazos a las víctimas y de esta manera hacerles creer situaciones que aprovechan para obtener información y materializar su delito.

Aunado a lo anterior, en la figura 13 se muestra gráficamente las pérdidas millonarias, resultado de estas modalidades utilizadas por los delincuentes durante la vigencia 2017.

Figura 13. Modalidades, casos reportados y pérdidas millonarias



Fuente: Centro Cibernético Policial. Informe Balance Cibercrimen en Colombia 2017. [En Línea]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_cibercrimen_2017.pdf

8.1 ATAQUES A ENTIDADES ESTATALES

A nivel de Gobierno se han presentado ataques informáticos de software malicioso producto de infección de malware y RAT (Herramientas de acceso remoto), que facilitan al delincuente en acceder a información del sector público, dinero y bases de datos, lo que generó pérdidas por más de 50 mil millones en Alcaldías nacionales.

En relación a Colombia existen ataques a diferentes Entidades Estatales en el país, como lo es el caso de la Alcaldía de Albania según lo informo revista Semana en la vigencia 2017[57], el mandatario Encargado Aurelio Efraín Arregocés Peñarredonda presuntamente haber tratado de desviar 22.000 millones de pesos del fondo de regalías a cuentas de ciberuelas en el país a través de la infección de un malware conocido como Trivia.

Es el caso de las elecciones populares, algunos como la candidata Hernández para la gobernación de Santander, difundió la intención de voto a través de redes sociales con una encuesta falsa, fue descubierto por el periódico El espectador[58], esto es muestra de otra forma de fraude por lo tanto el uso de redes sociales es frecuente para incentivar percepciones erróneas y obtener resultados sesgados.

En el estudio "Tendencias Cibercrimen en Colombia 2019-2020"[59] , liderado por el programa Seguridad Aplicada al Fortalecimiento Empresarial (SAFE) del Tanque de Análisis y Creatividad de las TIC (TicTac), la Cámara Colombiana de Informática y Telecomunicaciones (CCIT) y el Centro de Capacidades para la Ciberseguridad de Colombia (C4) de la Policía Nacional muestra el crecimiento del cibercrimen en Colombia del 54% para lo que va del año 2019 con 30.410 casos registrados respecto al año 2018 donde fueron gestionados 8.363 casos, todos estos casos fueron registrados por las empresas y la ciudanía en General a través de los diferentes canales de atención dispuestos por la Policía Nacional.

Para la vigencia 2019 las entidades más afectadas en Colombia por los delitos informáticos son:

- Pequeñas empresas (PYMES)
- Medianas empresas (PYMES)
- Grandes empresas
- Entidades financieras

El factor común de estas entidades es su ubicación en las principales ciudades de Colombia donde por lo general el número de habitantes y penetración de internet es mayor, por lo que se puede observar en la siguiente información las ciudades más afectadas:

---

[57] REVISTA SEMANA. El "regalito" de navidad que tiene sentado al alcalde de Albania en el banquillo de acusados [En línea], agosto 2017, [Consultado 15 febrero 2018]. Disponible en internet: <https://www.semana.com/Item/ArticleAsync/546433>

[58] El espectador. Ángela Hernández, candidata a Gobernación de Santander, difunde encuesta falsa. En línea. Disponible en internet: https://www.elespectador.com/elecciones2019/angela-hernandez-candidata-gobernacion-de-santander-difunde-encuesta-falsa-articulo-886883

[59] Cámara Colombiana de Informática y Telecomunicaciones. Tendencias del Cibercrimen en Colombia 2019-2020. [En Línea]. Disponible en internet: http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Tabla 4.Ciudades más afectadas por Ciberataques en Colombia

CIUDAD	No. CASOS
Bogotá D.C	5.308
Cali	1.190
Medellín	1.186
Barranquilla	643
Bucaramanga	397

Fuente: Cámara Colombiana de Informática y Telecomunicaciones. Tendencias del Cibercrimen en Colombia 2019-2020. [En Línea]. Disponible en: http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Las ciudades mencionadas en la Tabla 4 equivalen al 55% de casos registrados en Colombia.

Un dato importante que menciona el estudio son los incidentes y delitos informáticos más reportados en Colombia de los cuales el Phishing es el incidente más reportado con el 42% como se puede observar en la tabla 5 y el delito informático más denunciado es el hurto por medios informáticos con 31.058 casos registrados como se puede observar en la tabla 6.

Tabla 5. Incidentes informáticos más reportados

TIPO DE ATAQUE	% REPORTES
Phishing	42%
Suplantación de identidad	28%
Fraudes por pagos en línea	16%
Malware	14%

Fuente: Cámara Colombiana de Informática y Telecomunicaciones. Tendencias del Cibercrimen en Colombia 2019-2020. [En Línea]. Disponible en: http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Tabla 6. Delitos informáticos más denunciados

TIPO DE DELITO	No. CASOS
Hurto por medios informáticos	31.058
Violación a datos personales	8.037
Acceso abusivo a sistema informático	7.994

Transferencia no consentida de activos	3.425
Uso de software malicioso	2.387

Fuente: Cámara Colombiana de Informática y Telecomunicaciones. Tendencias del Cibercrimen en Colombia 2019-2020. [En Línea]. Disponible en: http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

Cerca del 90% de los ciberataques que se realizan a las empresas en Colombia son mediante la Ingeniería Social y las modalidades más utilizadas para el cibercrimen en Colombia son de Ataque BEC (Compromiso de Cuestas Empresariales), Rasomware, Ataque DDOS (Denegación de Servicio), Malware, Sim Swaapping (Secuestro de SIM CARD), Cryptojacking (Minería de Criptomonedas).

Durante el congreso internacional de tecnologías de la información y las comunicaciones – ANDICOM 2019[60] en su versión número 34, el Presidente de Colombia Iván Duque informo que el gobierno esta trabajando en la elaboración de un documento conpes con el cual sirva de guía para poder enfrentar el cibercrimen que afecta a todo tipo de organizaciones en el mundo.

[60] PRESIDENCIA DE LA REPUBLICA DE COLOMBIA. Presidente Duque anuncia documento Conpes para combatir la amenaza global del cibercrimen [En línea], septiembre 2019. Disponible en internet: https://id.presidencia.gov.co/Paginas/prensa/2019/Presidente-Duque-anuncia-documento-Conpes-para-combatir-la-amenaza-global-del-cibercrimen-190904.aspx

9. OPERACIÓN ENTIDADES ESTATALES

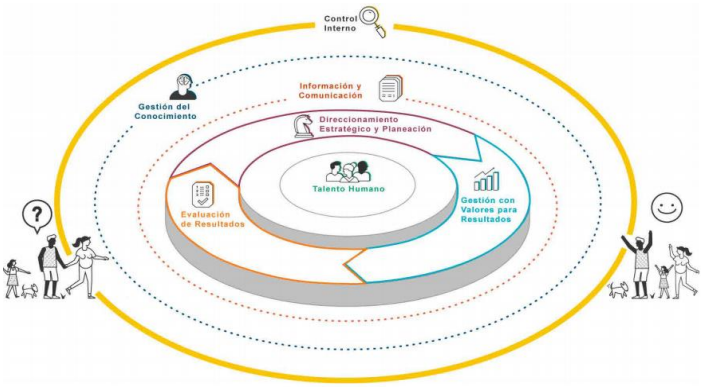
La Función Pública hace parte de los 24 sectores que componen la Rama Ejecutiva Nacional. La cual se define como “una entidad técnica, estratégica y transversal del Gobierno Nacional que contribuye al bienestar de los colombianos mediante el mejoramiento continuo de la gestión de los servidores públicos y las instituciones en todo el territorio nacional”.

Es decir, a través de esta organización se establecen lineamientos, planes, programas y proyectos que permiten a las Entidades Estatales enfocar su operación de manera eficiente para fortalecer su gestión, mejorar su desempeño y aumentar la confianza de la ciudadanía, así mismo buscando impartir directrices base para estas.

El Modelo de Planeación y gestión - MIPG[61] permite “dirigir, planear, ejecutar, controlar, hacer seguimiento y evaluar la gestión institucional de las entidades públicas, en términos de calidad e integridad del servicio para generar valor público”.

Como se observa en la figura 15, dicho modelo se basa en 7 dimensiones operativas (Talento humano, Direccionamiento Estratégico y Planeación, Gestión con valores para resultados, Evaluación de resultados, Información y comunicación, Gestión del Conocimiento, Control interno), es decir, cada uno de estas, contiene el conjunto de políticas, prácticas, elementos e instrumentos, que permiten desarrollar un proceso de gestión estratégica que se adapta a cada Entidad Estatal.

Figura 14. Dimensiones operativas del MIPG



Fuente: FUNCIÓN PÚBLICA. Modelo de Planeación y Gestión. [En Línea]. Disponible en: http://www.funcionpublica.gov.co/web/mipg/conocer-el-modelo

[61] FUNCIÓN PÚBLICA. Modelo de Planeación y Gestión. [En Línea]. Disponible en: http://www.funcionpublica.gov.co/web/mipg/conocer-el-modelo

10. TÉCNICAS ADECUADAS PARA CONTRARRESTAR LA INGENIERIA SOCIAL

A través de los métodos, políticas y herramientas que cada Entidad Estatal genera mediante la alineación el modelo MIPG para llevar la gestión institucional y teniendo en cuenta los capítulos anteriores; donde se evidencia los tipos de ataques, se aconseja tener en cuenta las siguientes acciones con el propósito de contrarrestar la Ingeniería Social.

Se hace necesario elaborar un diccionario de palabras técnicas asociadas con la ingeniería social, así como palabras de emergencia en caso de que los servidores públicos, contratistas y demás personal de la Entidad Pública detecten ataques de ingeniería social; a fin de reaccionar ante cualquier situación y la cual permita a las personas tener mayor rapidez para bloquear el ataque del delincuente. (Se puede replicar en el ámbito personal)

Que las Entidades Estatales incluyan en el Plan Institucional de Capacitaciones – PIC, temáticas asociadas con la ingeniera social, describiendo no solo sus conceptos, sino también detallando a los servidores públicos, contratistas y demás personal de la Entidad Pública los detalles de cómo los delincuentes están atacando mediante la Ingeniera Social. (Ataques mediante la observación, internet, teléfonos, correos electrónicos, entre otros)

Teniendo en cuenta los resultados de cada Entidad, con base al diagnóstico del componente de seguridad y privacidad de la Estrategia de Gobierno en Línea, es fundamental que se fabriquen planes de choque para neutralizar los ataques que pueden ser aprovechados por las vulnerabilidades detectadas.

Es necesario que todas las personas socialicen y compartan los conocimientos que puedan tener sobre Ingeniera Social a los demás, así mismo que se comunique con aquellos que se encuentran en su entorno, con el propósito de garantizar su protección y hasta la suya propia.

Generar claves seguras tanto en equipos, portátiles, smartphones, las cuales son propias e intransferibles. La mayoría de situaciones se presentan por que se suministra información a personas desconocidas, sitios web, correos electrónicos personales e institucionales que buscan una sola cosa, acceder a información confidencial.

Motivar a las personas para que exploren alternativas interiormente, así como acciones propias por sentido común y no se dejen envolver fácilmente por los delincuentes.

11. ETAPAS PLAN DE ACCIÓN

Para la definición de las etapas del plan de acción propuesto se tiene en cuenta el nuevo Modelo de Planeación y Gestión - MIPG de la Función Pública realizado por el Gobierno Nacional para las entidades públicas en Colombia, es importante mencionar que cada entidad es autónoma en la elaboración de los diferentes planes institucionales ya que pueden variar de una entidad a otra debido a las características propias de cada una de ellas. Con este plan de acción se pretende construir y entregar una herramienta a las Entidades Estatales para que puedan aplicar tanto en el ámbito Nacional y Territorial, a fin de estar preparados ante cualquier situación que se llegase a presentar en ataques de Ingeniería Social (Ver Figura 16).

Figura 15. Etapas Plan de Acción

Fuente: El autor.

En la tabla 7 se detalla cada una de las etapas propuestas en el plan de acción.

Tabla 7. Etapas del Plan de Acción

I-DIAGNÓSTICO	En esta etapa cada Entidad Estatal debe hacer una evaluación previa y conocer el estado en que la Entidad se encuentra frente a la Ingeniera Social.
II-ALINEACIÓN	En esta etapa, se debe tratar cada vulnerabilidad detectada conforme a los resultados anteriores y

	alinearla a dos ejes principales: (a). Modelo de Planeación y Gestión - MIPG, (b). Componente de Seguridad y Privacidad de la Información de la Estrategia de Gobierno en Línea.
III-CONSTRUCCIÓN	En esta etapa se debe construir y recrear situaciones reales, es decir un juego de roles donde los mismos servidores públicos contratistas o demás personal de la Entidad deben formar 3 grupos para cada situación (Atacante, Victima y Observador) basándose en las vulnerabilidades detectadas en la etapa uno.
IV-PREPARACIÓN	Teniendo en cuenta los resultados de la etapa anterior, es decir la socialización desde cada perspectiva, se abarca una visión general de las vulnerabilidades, así mismo se pueden detectar otras vulnerabilidades que no hayan sido contempladas en la etapa inicial, con el fin de contrarrestarlas.
V-FORTALECIMIENTO	Una vez consolidada todas las posibles vulnerabilidades de conformidad a la operación propia de cada Entidad y su acción preventiva, en esta última etapa se fomentará una cultura ante ataques de Ingeniería Social y se crean indicadores de seguimiento a fin de mantener en cero el indicador de ataques.

Fuente: El autor.

12. RESULTADOS E IMPACTOS ESPERADOS

Mediante uso adecuado que se dé al plan de acción, los resultados e impacto esperados serán los siguientes:

Es la ruta que permitirá a las Entidades Estatales prevenir la ingeniería Social, así como sentar las bases para la generación de una cultura organizacional frente a estos ataques.

Mediante la ejecución por etapas de este Plan de Acción propuesto, se garantiza confianza en la identificación total de las posibles vulnerabilidades, puesto que son acordes con cada Entidad, a su infraestructura, la seguridad física, el personal que labora, seguridad que tienen los sistemas informáticos, a los procesos internos, entre otros.

Este Plan permitirá una mayor organización tanto en las actividades a ejecutar, así como la delegación de responsabilidades, puesto que es cada área quien determina las posibles vulnerabilidades y sus acciones conforme a los recursos existentes, de tal manera que busquemos como propósito garantizar un mayor compromiso de todos, debido a que se lograra trascender organizacionalmente y personalmente.

Ayudará a prevenir los ataques, puesto que, mediante la capacitación y concientización a todos, permitirá bajar las cifras expuestas en capítulos anteriores, puesto que se contaría con bases sólidas para contrarrestar cualquier ataque y poder actuar anticipadamente.

La convicción que este plan de acción traerá beneficios y servirá como escudo ante cualquier ataque, a fin de demostrar su utilidad, así como evidenciar el impacto que tendrá con su implementación, puesto que hará a las Entidades Estatales unificar esfuerzos para desarrollar un lineamiento general.

Con la implementación del juego de roles propuesto para desarrollarse en el Plan de Acción, se logrará contar con un panorama amplio de cómo ve la situación el atacante, la víctima y la persona que está encargada de observar, puesto que todas estas perspectivas alimentaran la definición de acciones robustas que contemplen varios frentes.

Se genera un Plan de Acción como anexo, el cual contiene las etapas con cada una de sus actividades, responsables, fechas de inicio y fin, así como los recursos utilizados.

CONCLUSIONES

Por medio del estudio del estado del arte sobre la ingeniería social se logró evidenciar los factores que afectan las diferentes entidades a nivel mundial y a nivel Colombia los cuales dejan brechas que los delincuentes informáticos aprovechan para realizar ataques de tipo ingeniería social. Por lo tanto, se evidencio la falta de mecanismos que ayuden a contrarrestar los ataques mediante el uso de la ingeniería social al interior de estas entidades.

Las cifras analizadas sobre los diferentes ataques informáticos actuales que se estudiaron y expusieron a lo largo del presente documento, fueron una base fundamental para el desarrollo de este estudio, dichas cifras indican pérdidas millonarias en las diferentes entidades tanto privadas, publicas, gubernamentales y sin ánimo de lucro demostrando que las personas que trabajan en estas entidades carecen de capacitación y socialización sobre los diferentes delitos informáticos a los que están expuestos y no se preocupan por consultar, verificar o corroborar la información que un extraño, amigo o compañero (delincuente) está usando para manipularlos, lo cual facilita que se genere nuevos tipos de ataques y se lleve a cabo el delito el cual genera pérdidas económicas para las entidades.

Con base a la información recolectada y mencionada se logró realizar un estudio solido que permite evidenciar el impacto de la ingeniería social y como minimizarlo en las entidades estatales con el fin de evitar la pérdida de recursos financieros a causa de fallas como el factor humano.

En Colombia aún faltan mecanismos que permitan mayor control sobre la Ingeniería Social, debido a que esta técnica es compleja de evitar en algunas circunstancias porque llega a ser indetectable y silenciosa, ya que se presenta como una situación del común para la víctima que está siendo atacada por el delincuente. Al definir mecanismos acordes con las vulnerabilidades detectadas en la operación propia de cada Entidad Estatal, se establece una dirección segura que conlleva al éxito de prevenir posibles fallas de seguridad.

No existe un lineamiento o esquema formal que permita tener una ruta para que todos los servidores públicos, contratistas y demás personal que hacen parte de las Entidades Estales puedan avanzar y neutralizar todo sobre la Ingeniera Social y los diferentes tipos de ataques cibernéticos. Es por ello que se propone las diferentes etapas de un Plan de Acción como una herramienta guía que permita evitar o minimizar el impacto de la ingeniería social al interior de las diferentes entidades estatales.

RECOMENDACIONES

Teniendo en cuenta el desarrollo de este estudio, se recomienda:

Conforme al Plan de Acción propuesto por las entidades Estatales, posterior a su implementación, deben agruparse en mesas de trabajo con el fin de dialogar lecciones aprendidas a nivel Nacional y Territorial, a fin de robustecer un lineamiento general y de esta manera avanzar con el flagelo de la inseguridad.

Así mismo se recomienda que las personas participantes que conocen de primera mano las experiencias que afrontaron durante la ejecución del plan, realicen la socialización de los desafíos vividos a fin de generar los insumos necesarios para la construcción de un segundo plan de acción de ser necesario.

Priorizar y definir acciones que contrarresten aquellos ataques que tienen mayor impacto en las Entidades Nacionales y Territoriales para estructurar los procesos tanto internos como externos y su interacción.

Establecer mecanismos de participación ciudadana sobre la información que es utilizada y manejada por las Entidades Estatales, con el propósito de generar una cultura de seguridad, es decir una cultura ante ataques de Ingeniería Social.

Impulsar la creación piloto de un observatorio digital dedicado exclusivamente a las Entidades Nacionales y Territoriales, mostrando toda la información asociada con la Ingeniera social y todas las posibles vulnerabilidades a lo que están expuestos durante el manejo de información pública.

Promover campañas a nivel de las Entidades Nacionales y Territoriales con los casos relevantes y de mayor impacto que han afectado directa e indirectamente al interior de las mismas y evitar que sean reiterativos.

Se recomienda realizar capacitaciones a los funcionarios de las Entidades Nacionales y Territoriales sobre seguridad de la información donde se evidencie las diferentes formas que utilizan los delincuentes informáticos para tener acceso a la información con el fin de evitar el mayor número de afectaciones al interior de las entidades.

BIBLIOGRAFIA

ALEXANDER, Michael. Methods for Understanding and Reducing Social Engineering Attacks [En Línea]. SANS Institute InfoSec Reading Room, 2016. p. 2 Disponible en internet: https://www.sans.org/reading-room/whitepapers/critical/methods-understanding-reducing-social-engineering-attacks-36972

BERMUDES, Edilberto. Ingeniería social: un factor de riesgo informático inminente en la Universidad Cooperativa de Colombia sede Neiva. Monografía Especialista en Seguridad Informática. Neiva: Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas, Tecnología e Ingeniería [En línea], junio 2015. 116 p. Disponible en internet: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/3629/1/1075210015.pdf

BORGHELLO, Cristian. El arma infalible: la Ingeniería Social [En línea]. San Diego California: ESET. 2009. p.7. Disponible en internet: http://www.eset-la.com/pdf/prensa/informe/arma_infalible_ingenieria_social.pdf

BSI. Group México S de RL de CV. ISO/IEC 27001 – Gestión de Seguridad de la Información – Guía de Transición. 4p y 6p.

BYTE TI. La importancia y el riesgo del factor humano en la ciberseguridad. [En línea]. Madrid. 2017. Disponible en internet: https://www.revistabyte.es/publirreportaje/riesgo-factor-humano-la-ciberseguridad/.

CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias del Cibercrimen en Colombia 2019-2020. [En Línea]. Disponible en internet: http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/

CENTRO CIBERNÉTICO POLICIAL. [En Línea]. Disponible en internet: https://caivirtual.policia.gov.co/

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1273. (05, enero, 2009). Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones. Diario Oficial. Bogotá, D. C., 2009. no. 47.223. 4 p.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1336. (21, julio, 2009). Por medio de la cual se adiciona y robustece la Ley 679 de 2001, de lucha contra la

explotación, la pornografía y el turismo sexual con niños, niñas y adolescentes. Diario Oficial. Bogotá, D. C., 2009. no. 47.417. 8 p.

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. 34 p.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley 1712. (06, marzo, 2014). Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones. Diario Oficial. Bogotá, D. C., 2014. no. 49084. 314 p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 527. (18, agosto, 1999). Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones. Diario Oficial. Santafé de Bogotá, D.C.,1999. No.43.673. 19p.

COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 594. (14, julio, 2000). Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones. Diario Oficial. Santa Fe de Bogotá, D. C., 2000. no.44084. 9 p.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatuaria 1266. (31, diciembre, 2018). 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.47.219. 17 p.

COLOMBIA. CONGRESO DE LA REPUBLICA. Ley Estatutaria 1581. (17, octubre, 2012). Por la cual se dictan disposiciones generales para la protección de datos personales. Diario Oficial. Bogotá, D. C., 2012. no.48587. 167p.

COMPUTERWORLD COLOMBIA. Ataques en seguridad seguirán siendo protagonistas en2018. [En Línea]. Disponible en internet: https://computerworld.co/ataques-en-seguridad-seguiran-siendo-protagonistas-en-2018/

CONPES 10.24. En línea. Recuperado de: https://webcache.googleusercontent.com/search?q=cache:sHf7Q4ul6j0J:https://www.dnp.gov.co/CONPES/Documents/2019-10-24%2520Documento%2520CONPES%2520National%2520Policy%2520for%2520Digital%2520Trust%2520and%2520Security.pdf+&cd=1&hl=es-419&ct=clnk&gl=co#20

CORREA, Alejandro y ORREGO, Carlos Andrés, Marcela. The social engineering framework para el aseguramiento de PYME [En línea]. Trabajo de grado Ingeniero de Sistemas. Medellín: Universidad EAFIT. Escuela de Ingeniería, 2015. 61 p. Disponible en internet: https://repository.eafit.edu.co/handle/10784/8550

COSTANTINO, G.; LA MARRA, A.; MARTINELLI, F.; MATTEUCCI, I. CANDY: Un ataque de ingeniería social para filtrar información del sistema de infoentretenimiento. En Actas de la Conferencia de Tecnología Vehicular IEEE, Oporto, Portugal, del 3 al 6 de junio de 2018; pp. 1-5

DIGIWARE. Cibercrimen en Colombia. [En Línea]. Disponible en internet: http://www.digiware.net/sites/default/files/doc_digiware_infografias/Infografia-Cibercrimen-en-Colombia.png

EDWARDS M, LARSON R, GREEN B, RASHID A, BARON A. (2017). Búsqueda de oro: análisis automático de superficies de ataque de ingeniería social en línea. Comput Secur. 2017.

ESET Security Report Latinoamérica 2017 [En línea]. ESET, 2017. [Consultado 18 febrero 2018]. Disponible en internet: https://www.welivesecurity.com/wp-content/uploads/2017/04/eset-security-report-2017.pdf

ESTRATEGIA DE GOBIERNO EN LÍNEA. Índice de Gobierno Digital [En Línea]. Disponible en internet: http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7651.html

FERREIRA, A., COVENTRY, L. Y LENZINI, G. Principios de persuasión en ingeniería social y su uso en phishing. Lecture Notes in Computer Science (incluidas las subseries Lecture Notes in Artificial Intelligence y Lecture Notes in Bioinformatics) (2015)

FUNCIÓN PÚBLICA. Modelo de Planeación y Gestión. [En Línea]. Disponible en internet: http://www.funcionpublica.gov.co/web/mipg/conocer-el-modelo

GALLO, José María. La información como activo estratégico de la empresa [En línea], mayo 2014. [Consultado 18 febrero 2018]. Disponible en internet: https://businessvalueexchange.com/es/2014/05/05/la-informacion-como-activo-estrategico-de-la-empresa/

GUTIÉRREZ, D. M. J. A., & Pagés, A. C. Planificación y gestión de proyectos informáticos [En Línea]. Alcalá de Henares, ES: Servicio de Publicaciones. Universidad de Alcalá 2008. Disponible en internet: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10280334&p00=pmi+pmbok+5

HEARTFIELD R, LOUKAS G. (2018). Detectando ataques semánticos de ingeniería social con el eslabón más débil: implementación y evaluación empírica de un marco humano como sensor de seguridad. [En línea]. Recuperado de: http://www.sciencedirect.com/science/article

ICONTEC. Norma Técnica Colombiana NTC 1486. Documentación. Presentación de Tesis, trabajos de grado y otros trabajos de investigación [En Línea]. ICONTEC 2008. Disponible en internet: http://www.unipamplona.edu.co/unipamplona/portalIG/home_15/recursos/01_general/09062014/n_icontec.pdf

ICONTEC. NORMA TÉCNICA COLOMBIANA NTC-ISO/IEC27001-por el Instituto Colombiano de Normas Técnicas y Certificación [En Línea]. Disponible en internet: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

JUNGER M, MONTOYA L, OVERINK FJ El cebado y las advertencias no son efectivos para prevenir ataques de ingeniería social. Comput Hum Behav. 2017. [En línea]. Recuperado de: https://doi.org/10.1016/j.chb.2016.09.012

KARPERSKY LAB. Ciberamenaza Mapa Tiempo Real [En Línea]. Disponible en internet: https://cybermap.kaspersky.com/es/stats/

MARCHETTI, F. PIERAZZI, A. GUIDO Y M. COLAJANNI, “Contrarrestar las amenazas persistentes avanzadas a través de la inteligencia de seguridad y análisis de datos grandes”, en Cyber Con fl ict (CyCon), 2016 8ª Conferencia Internacional sobre. IEEE, 2016

MINTIC. Ingeniería Social. [En línea]. Bogotá D.C. S.F. Disponible en internet: http://www.mintic.gov.co/portal/604/w3-article-18800.html.

MONSALVE, JAIME. CIBERSEGURIDAD: PRINCIPALES AMENAZAS EN COLOMBIA (INGENIERÍA SOCIAL, PHISHING Y DoS). Artículo. [En línea]. Recuperado de: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4663/00004883.pdf?sequence=1&isAllowed=y

PRESIDENCIA DE LA REPUBLICA DE COLOMBIA. Presidente Duque anuncia documento Conpes para combatir la amenaza global del cibercrimen [En línea], septiembre 2019. Disponible en internet: https://id.presidencia.gov.co/Paginas/prensa/2019/Presidente-Duque-anuncia-documento-Conpes-para-combatir-la-amenaza-global-del-cibercrimen-190904.aspx

REVISTA SEMANA. El “regalito” de navidad que tiene sentado al alcalde de Albania en el banquillo de acusados [En línea], agosto 2017, [Consultado 15 febrero 2018]. Disponible en internet: https://www.semana.com/Item/ArticleAsync/546433

RUBÉN, Ramiro. 25 Tipos de ataques informáticos y cómo prevenirlos [En Línea]. Ciberseguridad 2018. Disponible en internet: https://ciberseguridad.blog/25-tipos-de-ataques-informaticos-y-como-prevenirlos/

SABOUNI S, CULLEN A, ARMITAGE L. Un marco preliminar de radicalización basado en técnicas de ingeniería social. Conferencia internacional de 2017 sobre conciencia cibernética situacional, análisis y evaluación de datos (Cyber SA). Londres, Reino Unido: IEEE. 2017.

SALAZAR, Natalia y GONZALEZ, Marcela. Phishing: la automatización de la ingeniería social. Trabajo de grado Ingeniero de Sistemas. Medellín: Universidad EAFIT. Escuela de Ingeniería [En línea]. Disponible en internet: https://repository.eafit.edu.co/bitstream/handle/10784/2443/Salazar_Natalia_2007.pdf?sequence=1&isAllowed=y.

SAMAR A Y GEORGE R. Vulnerabilidad a la Ingeniería Social en Social Redes: un marco propuesto centrado en el usuario. Artículo. Traducción [En línea]. Recuperado de: https://pure.strath.ac.uk/ws/portalfiles/portal/63205006/Albladi_Weir_ICCCF2016_Vulnerability_to_social_engineering_in_social_networks.pdf

SCHAAB P, BECKERS K, PAPE S. Mecanismos de defensa de ingeniería social y estrategias de formación contrarias. Inf Comput Secur. 2017 [En línea]. Recuperado de: https://doi.org/10.1108/ICS-04-2017-0022

SOLANAS, Carmen. Estudio de las técnicas de la Ingeniería Social usadas en ataques de Ciberseguridad y Análisis Sociológico. Trabajo de grado Ingeniería de Tecnologías y Servicios de Telecomunicación. Madrid: Universidad Politécnica de Madrid. Escuela técnica superior de Ingenieros de Telecomunicación [En línea]. septiembre 2015. 56 p. Disponible en internet: http://oa.upm.es/37773/1/PFC_MARIA_DEL_CARMEN_SOLANAS_VENRELL_2015.pdf

SPINAPOLICE, Matthew. Mitigating the risk of social engineering attacks [En Línea]. Rochester Institute of Technology RIT Scholar Works, 2011. Disponible en internet: http://scholarworks.rit.edu/cgi/viewcontent.cgi?article=1397&context=theses

TECNÓSFERA – El Tiempo. A diario se registran 542.465 ataques informáticos en Colombia. [En Línea], septiembre 2017. [Citado en 22 de febrero de 2018]. Disponible en internet: https://www.eltiempo.com/tecnosfera/novedades-tecnologia/informe-sobre-ataques-informaticos-en-colombia-y-al-sector-financiero-

135370

WELIVESECURITY. Editor de ESET.com. 5 Cosas que debes saber sobre la Ingeniería Social. - Noticias, opiniones y análisis de la comunidad de seguridad de ESET. [En Línea]. 2016. Disponible en internet: https://www.welivesecurity.com/la-es/2016/01/06/5-cosas-sobre-ingenieria-social/

X. Wang, K. Zheng, X. Niu, B. Wu y C. Wu, "Detección de comando y control en amenazas persistentes avanzadas basadas en acceso independiente", en Comunicaciones (ICC), Conferencia Internacional IEEE 2016 en IEEE, 2016

ZAKHAROVA, L. "La communication totalitaire, une technique d'ingénierie sociale", Books and Ideas, 23 mars 2011. ISSN: 2105-3030 [En línea]. Disponible en internet: http://www.laviedesidees.fr/La-communication-totalitaire-une.html

ANEXOS

Anexo A. Plan de acción propuesto

EVENTOS PRINCIPALES	RESPONSABILIDAD		CALENDARIO		RECURSOS	MONITOREO Y CONTROL
	PRIMARIA	APOYO	INICIO	FIN		
DIAGNÓSTICO	*OBJETIVO*	*Evaluar previamente para conocer el estado en que la Entidad se encuentra frente a la Ingeniera Social*				
Desarrollar un cuestionario para saber si los servidores públicos conocen todo sobre la Ingeniería Social	Secretaria TIC, Oficina TIC o quien haga sus veces	Personal TIC	oct-2020	oct-2020	Humanos, tecnológicos, físicos	Secretaria Administrativa o quien haga sus veces - Oficina de Calidad y Control
Aplicar el cuestionario a toda la Entidad	Secretaria Administrativa o quien haga sus veces	Secretaria TIC, Oficina TIC o quien haga sus veces	nov-2020	nov-2020		
Consolidar datos	Secretaria TIC, Oficina TIC o quien haga sus veces	Personal TIC	dic-2020	dic-2020		
Socializar resultados a todos los Secretarios de Despacho o quien haga sus veces	Secretaria Administrativa o quien haga sus veces	Secretaria TIC, Oficina TIC o quien haga sus veces	dic-2020	dic-2020	Humanos, tecnológicos, físicos	Secretaria Administrativa o quien haga sus veces - Oficina de Calidad y Control
ALINEACIÓN	*OBJETIVO*	*Alinear vulnerabilidades detectadas con el Modelo de Planeación y Gestión y Estrategia Gobierno en Línea*				
Tomar resultados de la etapa anterior y detectar las posibles vulnerabilidades	Todas las dependencias deben involucrarse y designar una persona líder por cada una de ellas		ene-2021	ene-2021	Humanos, tecnológicos, físicos	Secretario de Despacho de cada dependencia

Conforme a los recursos propios de cada Entidad Estatal, definir las acciones preventivas o correctivas					Financieros, humanos, tecnológicos, físicos	
Alinear cada acción con el Modelo de Planeación y Control a fin de mantener una arquitectura armónica para cada Entidad, a fin de evitar el sobredimensionamiento de recursos existentes			feb-2021	feb-2021	Humanos, tecnológicos, físicos	
Alinear cada acción con el componente de Seguridad y privacidad de la Información de la Estrategia de Gobierno en Línea, con el propósito de garantizar en paralelo su ejecución					Humanos, tecnológicos, físicos	
CONSTRUCCIÓN	*OBJETIVO*	*Construir y recrear situaciones reales mediante un juego de roles (Atacante, Victima y Observador)*				
Seleccionar por cada dependencia u área 3 grupos (Atacante, Victima y Observador)	Personal delegado asignado por Jefe de Despacho	Secretario de Despacho de cada dependencia	mar-2021	abr-2021	Financieros, humanos, tecnológicos, físicos	Secretaria Administrativa, Secretaria TIC o quien haga sus veces
Diseñar y recrear las situaciones de acuerdo a las vulnerabilidades detectadas	Personal delegado asignado por Jefe de Despacho					
Entregar a cada grupo los perfiles asociados, describiendo las tareas a desarrollar	Secretaria Administrativa o quien haga sus veces	Personal TIC				
Socializar resultados una vez finalice el juego de roles	Personal delegado asignado por Jefe de Despacho					
PREPARACIÓN	*OBJETIVO*	*Detectar otras vulnerabilidades que no hayan sido contempladas en la etapa inicial*				

Consolidar todas las perspectivas por dependencias y por perfil (Atacante, Victima y Observador)	Secretaria Administrativa o quien haga sus veces	Personal TIC	may-2021	may-2021	Humanos, tecnológicos, físicos	Secretaria Administrativa o quien haga sus veces
Verificar si las vulnerabilidades detectadas inicialmente están en su totalidad, de lo contrario incluirlas	Todas las dependencias deben involucrarse, verificando cada resultado					Secretario de Despacho de cada dependencia
Definir acciones preventivas para prepararse ante ataques	Personal delegado asignado por Jefe de Despacho	Secretario de Despacho de cada dependencia	jun-2021	jun-2021	Financieros, humanos, tecnológicos, físicos	Secretario de Despacho de cada dependencia
FORTALECIMIENTO	*OBJETIVO*	*Fomentar una cultura ante ataques de Ingeniería Social*				
Establecer indicadores de seguimiento a fin de garantizar el cumplimiento de las acciones	Secretario de Despacho de cada dependencia	Secretaria Administrativa o Planeación	jun-2021	jun-2021	Humanos, tecnológicos, físicos	Secretaria Administrativa o quien haga sus veces
Realizar capacitaciones a fin de concientizar a todo el personal de la Entidad	Secretaria Administrativa o quien haga sus veces		jul-2021	jul-2021	Financieros, humanos, tecnológicos, físicos	Secretaria Administrativa o quien haga sus veces
Crear diccionario de datos con palabras asociadas a la Ingeniería Social y palabras de emergencia	Secretaria TIC, Oficina TIC o quien haga sus veces		oct-2021	jul-2021	Humanos, tecnológicos, físicos	Secretaria TIC, Oficina TIC o quien haga sus veces
Generar una directriz Institucional	Alta Dirección	Secretario de Despacho de cada dependencia	jul-2021	ago-2021	Financieros, humanos, tecnológicos, físicos	Alta Dirección