ESTUDIO MONOGRÁFICO: IMPACTO DE LA TÉCNICA DE ATAQUE DE *PHISHING* EN COLOMBIA DURANTE LOS ÚLTIMOS CINCO AÑOS

JENIFFER ANDREA RUEDA QUINTERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

ESTUDIO MONOGRÁFICO: IMPACTO DE LA TÉCNICA DE ATAQUE DE *PHISHING* EN COLOMBIA DURANTE LOS ÚLTIMOS CINCO AÑOS

JENIFFER ANDREA RUEDA QUINTERO

Monografía

Director

Mariano Esteban Romero Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ
2020

Nota de aceptación

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

_____

Firma del jurado

_____

_____

Firma del jurado

Bogotá D.C Diciembre 2020

Dedicatoria

Dedicado a mi hija Sara Díaz Rueda, quien es el motivo de mi lucha día tras día, con su alegría y entusiasmo me llena de vida e ilusión, en seguir creciendo constantemente siempre fortalecida de la mano de Dios y guiada por la llena de gracia, la Virgen María.

A mi mamá, mis hermanos y grandes amigos que pusieron un grano de arena, ellos siempre dándome su apoyo incondicional, merecen esta dedicatoria.

Agradecimientos

Agradezco a Dios y a la Virgen, esta oportunidad y a todas las personas que me ayudaron en el proceso.

Gracias a la Procuraduría General de la Nación, al Doctor Juan Carlos Novoa y la Doctora María Eugenia Carreño por su gran apoyo, a la Universidad Nacional Abierta y a Distancia UNAD, a los docentes de la Especialización en Seguridad Informática, especialmente al profesor Alexander Larrahondo por su compromiso con la universidad y los estudiantes.

Gracias al Director Mariano Romero, por toda su colaboración y disposición. Y finalmente gracias infinitas a mis grandes amigos, Roberto Salinas; Manuel Camargo; Luis Fernando Súa y William Devia. Sin ustedes no lo hubiera logrado. ¡Gracias!

CONTENIDO

pág.

TABLA DE FIGURAS

pág.

LISTA DE TABLAS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

ACTIVO DE INFORMACIÓN: “recurso de valor para el desarrollo de la actividad propia de la Institución que incluye la gestión de la información, el software para su tratamiento y los soportes físicos y lógicos de la información”[1].

AMENAZA: “se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información. Las amenazas surgen a partir de la existencia de vulnerabilidades, es decir que una amenaza sólo puede existir si existe una vulnerabilidad que pueda ser aprovechada, e independientemente de que se comprometa o no la seguridad de un sistema de información”[2].

AUTENTICIDAD: “la legitimidad y credibilidad de una persona, servicio o elemento debe ser comprobable”[3].

CONFIDENCIALIDAD: “uno de los tres principios básicos de la implementación de la seguridad de la información. La confidencialidad implica que debe protegerse la información de forma tal que sólo sea conocida por las personas autorizadas y se la resguarde del acceso de terceros”[4].

DELITO INFORMÁTICO: “es toda acción típica, antijurídica y culpable, para cuya consumación se usa la tecnología computacional o se afecta a la información contenida en un sistema de tratamiento autorizado de la misma”[5].

DISPONIBILIDAD: “uno de los tres principios básicos (los otros dos son el principio de integridad y el de confidencialidad) de la implementación de la seguridad de la información. La disponibilidad implica que debe protegerse la información de forma

---

[1] UNIVERSIDAD NACIONAL DE LUJAN, Departamento de seguridad informática: Activo de Información. [En Línea]. [Consultado: 19 de febrero de 2019]. Disponible en http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/22

[2] UNIVERSIDAD NACIONAL DE LUJAN, Departamento de seguridad informática: Amenaza. [En Línea]. [Consultado: 19 de febrero de 2019]. Disponible en http://www.seguridadinformatica.unlu.edu.ar/?q=node/12)

[3] ERB, Markus. Gestión de Riesgo en la Seguridad Informática. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://protejete.wordpress.com/about/

[4] UNIVERSIDAD NACIONAL DE LUJAN, Departamento de seguridad informática: Confidencialidad. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/3

[5] VÁSQUEZ, Magaly y CHACÓN, Nelson. Ciencias penales, Citado por: JIJENA LEIVA, Renato Javier. La criminalidad Informática. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://books.google.com.co/books?id=-jVch6LUPaQC&pg=PA582&dq=definici%C3%B3n+delito+informatico&hl=es&sa=X&ved=0ahUKEwi3r9Xl7MrgAhVrw1kKHX82DToQ6AEILjAB#v=onepage&q=definici%C3%B3n%20delito%20informatico&f=false

tal que se pueda disponer de ella para su gestión en el tiempo y la forma requeridos por el usuario"[6].

DERECHO INFORMÁTICO: "ciencia y rama autónoma del Derecho que abarca el estudio de las normas, jurisprudencias y doctrinas relativas al control y regulación de la informática en aspectos como la regulación del medio informático en su expansión y desarrollo, y la aplicación idónea de los instrumentos informáticos"[7].

INTERNET: "red informática mundial, descentralizada, formada por la conexión directa entre computadoras mediante un protocolo especial de comunicación"[8].

INFORMÁTICA: "conjunto de conocimientos científicos y técnicas que hacen posible el tratamiento automático de la información por medio de computadoras"[9].

RIEGOS INFORMÁTICOS: "incertidumbre existente por la posible realización de un suceso relacionado con la amenaza de daño respecto a los bienes o servicios informáticos como por ejemplo los equipos informáticos, periféricos, instalaciones, proyectos programas de cómputo, archivos información datos confidenciales, responsabilidad civil que estos ocasionan frente a terceros por la prestación de un servicio informático"[10].

SPEAR PHISING: "es una variante del *phishing* y consiste en el envío de mensajes, generalmente por correo electrónico, específicos y personalizados a un grupo de personas determinado. Esta es la principal diferencia respecto al *phishing* tradicional por email, que consistía en el envío de un mismo correo electrónico de forma masiva y al azar a millones de usuarios"[11].

PHISHING: "el *phishing* es una técnica de ingeniería social utilizada por los delincuentes para obtener información confidencial como nombres de usuario,

---

[6] UNIVERSIDAD NACIONAL DE LUJAN, Departamento de seguridad informática: Disponibilidad. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/2

[7] ECURED, Derecho Informático. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://www.ecured.cu/Derecho_inform%C3%A1tico

[8] RAE, Internet. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://dle.rae.es/?id=LvskgUG

[9] Ibíd., p. Informática.

[10] TÉLLEZ VALDÉS, Julio. Contratos Informáticos. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://books.google.com.co/books?id=m-MwmFPGCxQC&pg=PA33&dq=QUE+ES+riesgo+informatico&hl=es-419&sa=X&ved=0ahUKEwjQ2tOx9JPgAhXpY98KHUP8AKgQ6AEIKDAA#v=onepage&q=QUE%20ES%20riesgo%20informatico&f=false

[11] S21sec, Spear phishing. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://www.s21sec.com/es/blog/2013/05/glosario-de-terminos-que-es-el-spear-phishing/

contraseñas y detalles de tarjetas de crédito haciéndose pasar por una comunicación confiable y legítima”[12].

SMISHING: “robo de información de los usuarios, por medio de mensajes de texto en dispositivos móviles”[13].

TABNABBING: “es el nuevo método de *Phishing* en Internet, Aza Raskin (quien descubrió el método) muestra como la acostumbrada navegación por pestañas puede convertirnos en víctimas de un ataque de *phishing* más ingenioso y sofisticado. El método se centra en las pestañas abiertas en el navegador y las páginas visitadas por el usuario anteriormente”[14].

TELECOMUNICACIÓN: “sistema de transmisión y recepción a distancia de señales de diversa naturaleza por medios electromagnéticos”[15].

TRAZABILIDAD: “aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento”[16].

VISHING: “el *vishing* es una nueva estafa que pretende suplantar la identidad del afectado a través de VoIP (*Voice over IP*), recreando una voz automatizada semejante a la de las entidades bancarias. El Grupo de Delitos Telemáticos de la Guardia Civil alerta en su portal de esta nueva variante de estafa cuyo término proviene de la unión de dos palabras: *voice* y *phishing*”[17].

WHALING: “en seguridad informática se denomina *whaling* a las técnicas de *phishing* dirigidas contra objetivos de alta importancia dentro de una organización (altos directivos de empresa, políticos, etc.) o simplemente de gran transcendencia social (cantantes, artistas, famosos, etc.)”[18].

---

[12] SEGU.INFO, Phishing. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://www.segu-info.com.ar/malware/phishing.htm

[13]MARTÍNEZ, Carlos, *et al*. Seguridad por capas frenar ataques de Smishing. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en Dialnetdialnet.unirioja.es

[14] MAESTROS DEL WEB, Tabnabbing. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en http://www.maestrosdelweb.com/que-es-tabnabbing-phishing-robo-identidad/

[15] RAE, Telecomunicación. [En Línea]. [Consultado 20 de febrero de 2019]. Disponible en https://dle.rae.es/?id=ZLVO47g

[16] QUIROZ, Jhon Henry y FORERO CRUZ, William. Diseño de Recomendaciones de Seguridad Informática sobre los Activos de Información Críticos de la Empresa Gran Tierra Energy Colombia - Seccional Bogotá. [En Línea]. [Consultado 20 de febrero de 2019]. Disponible en repository.ucatolica.edu.co

[17] BBVA, vishing. [En Línea]. [Consultado 20 de febrero de 2019]. Disponible en https://www.bbva.com/es/vishing-la-imaginacion-los-estafadores-no-limites/

[18] SECURIZANDO, Whaling. [En Línea]; [Consultado: 20 de febrero de 2019]. Disponible en https://securizando.com/whaling/

RESUMEN

La presente monografía es un estudio bibliográfico que, luego de indagar el impacto causado en Colombia, durante los últimos cinco años por la técnica del *phishing*, propone estrategias para mitigar dicho impacto. El *phishing* hace parte de las técnicas de ingeniería social; según el artículo, publicado por Avast[19], el *phishing* electrónico consiste en enviar un email aparentemente seguro, el cual, lleva en su contenido un *link*. Estos correos electrónicos solicitan amablemente que actualice, valide o confirme la información de una cuenta, sugiriendo a menudo que existe algún problema. Posteriormente, se redirige a una página web falsa y se le embauca para que facilite información sobre su cuenta, lo que puede provocar el robo de su identidad. La función del *phishing* es lograr que la víctima caiga en el engaño.

En el desarrollo de esta monografía se describe qué es el *phishing*, se presentan algunas de las herramientas que usan los delincuentes para lograr hacer este tipo de ataques en sus diferentes variedades. Se da a conocer los últimos reportes publicados por las entidades oficiales encargadas de la ciberseguridad en Colombia, como lo es el Centro Cibernético Policial e información de la Fiscalía General de la Nación y se proponen estrategias para mitigar dicho impacto, analizando los datos que dan a conocer el impacto de *phishing* en Colombia durante los últimos cinco años, asimismo se identifican los sectores más afectados, la modalidad más usada y algunos otros datos relevantes. Se exponen, igualmente, algunos casos reales ocurridos en Colombia y se analiza según la ley 1273 de 2009 “De la protección de la información y de los Datos”, donde se hace referencia al *phishing* como delito en Colombia. Finalmente, se realizan algunas recomendaciones para evitar ser víctimas de esta modalidad de ciberataque.

PALABRAS CLAVES: *phishing*, delitos informáticos, seguridad informática, gestión de riesgos, buenas prácticas.

[19] BELCIC, Iván. ¿Qué es exactamente el phishing? [En Línea]. Avast. Agosto 2018 [Consultado: 20 de febrero de 2019]. Disponible en https://www.avast.com/es-es/c-phishing

INTRODUCCIÓN

En la actualidad, la tecnología, el internet, las telecomunicaciones y la informática han avanzado a pasos agigantados, trayendo consigo grandes ventajas y beneficios para la humanidad. Tanto es así que, hoy en día se produciría un caos mundial si los estados y las empresas no tuvieran servicio de internet.

Sin embargo, de igual forma representan grandes riesgos y problemáticas para la seguridad informática, hasta el punto de crear la necesidad de desarrollar acuerdos internacionales para tomar medidas y poner los ojos en el concepto de la ciberseguridad. Por tanto, algunos gobiernos han entendido la importancia de proteger la información; ya que este es el activo más importante para cualquier entidad pública, privada o incluso para una persona del común. Con base en lo anterior, nacieron los pilares de la seguridad de la información, los cuales son: integridad, confidencialidad, disponibilidad, autenticidad y trazabilidad.

Así las cosas, es posible definir los pilares de la información en los siguientes términos: a. ***La integridad***, como la información que de principio a fin no ha sido alterada en ninguna manera; b. ***La confidencialidad,*** hace referencia a que, la información sea conocida únicamente por la entidad autorizada para tener acceso a esta información; c. ***La disponibilidad,*** es la información que, siempre que se necesite se encuentra disponible; d. ***La autenticidad,*** es el uso de usuario y contraseña para su identificación y de esta manera no se puede negar la responsabilidad en el manejo de la información y; e. ***La trazabilidad,*** es la evidencia o el registro del traspaso de información de un usuario a otro.

Por tanto, teniendo claridad en estos conceptos, es indispensable hablar sobre los delitos y el derecho informáticos, para dar un poco más de claridad sobre los riesgos y problemáticas mencionadas anteriormente. Los delitos informáticos son comportamientos o acciones ilícitas que se realizan por medio de los sistemas de información y por ende la importancia del derecho informático que toma las medidas legales pertinentes para sancionar este tipo de delitos. Los ciberdelincuentes tienen como objetivo dañar, hurtar, estafar e interceptar los sistemas informáticos, usando como medio las Tecnologías de la Información y la Comunicación - TIC.

En esta monografía se realiza un estudio bibliográfico con el fin de conocer el impacto del *phishing* en Colombia durante los últimos cinco años y de acuerdo con ello, proponer controles para mitigar este ataque informático. En el desarrollo de la monografía se da a conocer qué es el *phishing*, como se produce, cuáles son sus consecuencias, entre otros conceptos que son relevantes para abordar este tema de forma eficaz.

1. DEFINICIÓN DEL PROBLEMA

1.1 ANTECEDENTES

La técnica del *phishing*, comienza a ser conocida públicamente, aproximadamente en el año 1996. Esta palabra nace de la similitud con *fishing* (pescar) ya que, literalmente consiste en pescar a un usuario que caiga en la red, para recibir un beneficio de forma ilícita o realizar algún daño informático.

Esta técnica ha venido creciendo muy rápidamente a nivel mundial, así mismo su impacto económico y social, debido a que, tiene diferentes alcances. Inicialmente se consideraba que estaba limitado a realizar suplantación de identidad, robo de dinero y captura de datos por diferentes medios. Pero hoy en día se usa como una herramienta para realizar daños mayores, estos son, realizados por otros ciberataques como el *ransomware, malware*, ataque *Business Email Compromise* - BEC y entre otros.

Muestra de ello, es el ataque de *phishing* que recibió una de las empresas más conocida a nivel mundial de intercambio de criptomonedas, *Binance,* en mayo del 2019. Este ciberataque conllevó la pérdida de 7.000 bitcoines valorados en 40 millones de dólares. Adicionalmente, el informe *State of the Phish* elaborado por *Proofpoint*[20] indica que, el 55% de las organizaciones de todo el mundo se enfrentaron por lo menos a un ataque de phishing exitoso en 2019.

Según un informe de kaspersky[21], en la cumbre Latinoamericana de Ciberseguridad, se informó que se registran 45 ataques por segundo en América Latina y que fueron bloqueados 92 millones de accesos a sitios falsos de phishing, es decir que, evitaron que tres usuarios latinoamericanos fueran víctimas de mensajes de phishing, de igual forma, se estableció que Brasil es el país con más ataques de phishing a nivel mundial, seguido por Venezuela. Lo anterior, durante el periodo de julio de 2018 a julio de 2019.

[20] PROOFPOINT, State of the Phish [en línea]. 2020. [Consultado: 07 de octubre de 2020]. Disponible en: https://www.proofpoint.com/sites/default/files/2020-06/pfpt-es-state-of-the-phish-2020-reports-a4.pdf

[21] SD, Alberto. Kaspersky registra 45 ataques por segundo en América Latina [en línea]. KASPERSKY. 2019. [Consultado: 07 de octubre de 2020]. Disponible en: https://latam.kaspersky.com/blog/kaspersky-registra-45-ataques-por-segundo-en-america-latina/15274/

El informe de Tendencias del Cibercrimen en Colombia 2019-2020[22], indica que, el 90% de los ciberataques dirigidos a empresas en Colombia se deben a la ingeniería social. El *phishing* con el 42%, es el más reportado junto con la suplantación de identidad con el 28%, el envío de *malware* 14% y los fraudes en medios de pago en línea con el 16%.

1.2 DESCRIPCIÓN

En la actualidad, el uso de la tecnología se ha convertido en una necesidad para los colombianos por la facilidad que brinda para realizar pagos y compras online, comunicarse con la familia y amigos, trabajar desde casa con la opción de teletrabajo y /o estudiar de manera virtual, entre otros.

Sin embargo, esta facilidad trae consigo una mayor exposición a los delitos informáticos y quienes los cometen son denominados como ciber-criminales, los cuales, haciendo uso de vulnerabilidades de los sistemas informáticos, dispositivos digitales, redes y el desconocimiento y/o descuido de las personas, acceden para tomar el control del sistema, causar daños, denegar servicios, robar dinero, secuestrar información, acceder de forma abusiva al sistema e información confidencial, etc.

Una de las metodologías que usan los cibercriminales para acceder de forma abusiva a la información es el phishing, que es una metodología que no requiere de grandes conocimientos técnicos, a diferencia de otros ataques informáticos, ya que su método principal es engañar a su víctima usando el envío de correos electrónicos con links y páginas web falsas, haciéndole creer a la víctima que la página suplantada es la página original. Los que realizan esta práctica son conocidos generalmente como *phishers* (cibercriminal que practica el *phishing*). Lo anterior, para suplantar páginas de los bancos y solicitar actualización de los datos, de esta manera logran realizar robos online y acceder a información confidencial. Otra forma común de engañar a sus víctimas es prometiendo algún empleo o promocionando alguna forma de ganar dinero de forma fácil, cabe resaltar que, según la información publicada por la casa de antivirus PANDA[23], las vías de ataque se están multiplicando, ahora no sólo se usan correos electrónicos para cometer estos delitos sino también, se utilizan redes sociales como Facebook.

---

[22] POLICIA NACIONAL y CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias Cibercrimen Colombia 2019-2020 [en línea]. Bogotá. Octubre 29 del 2019. 36 páginas. Primera edición [Consultado: 12 de julio de 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

[23] PANDA. 10 consejos Para Evitar Ataques De Phishing. [En línea]. Febrero de 2016. [Consultado:12 de mayo de 2018]. Disponible en https://www.pandasecurity.com/spain/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/

El *phishing* ha afectado la economía de las empresas colombianas. Según la Policía Nacional[24], las ciudades más afectadas son: Bogotá, Cali, Medellín, Barranquilla y Bucaramanga; siendo Bogotá la ciudad más afectada con 5.308 casos. Así pues, en Colombia el monto promedio de las cifras de pérdidas por ataque puede oscilar entre 300 millones y 5.000 millones de pesos, según el tamaño de la empresa afectada.

1.3 FORMULACIÓN

El aumento del *phishing* en personas y empresas en Colombia ha tenido un impacto negativo en términos económicos y sociales, según un estudio realizado por el Banco Interamericano de Desarrollo - BID, el Ministerio de Tecnologías de la Información y las Comunicaciones y la Organización de los Estados Americanos-OEA; llamado Impacto de los Incidentes de Seguridad Digital en Colombia 2017.

Una problemática relevante que identifica el estudio se produce en las empresas del sector privado, especialmente las microempresas o empresas pequeñas con respecto a las empresas grandes. Ya que, cuando son víctimas de incidentes de seguridad entre unas y otras no se puede dimensionar la afectación real a su patrimonio y activos de información. Lo anterior, por la baja inversión en seguridad digital de las microempresas. Por el contrario, las empresas grandes que invierten en seguridad digital logran identificar más incidentes de seguridad, esto permite conocer las mejoras que se deben realizar y cómo actuar frente a estos ataques, y, por tanto, tener claridad sobre las grandes pérdidas que podría sufrir la empresa si llegara a realizarse un incidente de seguridad.

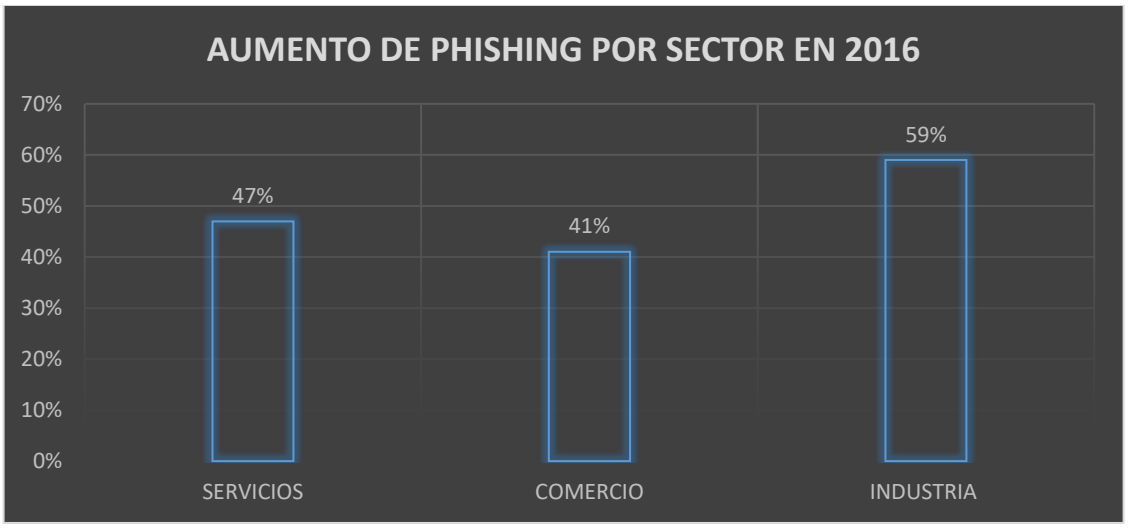
El estudio también permite identificar la necesidad de asignar un cargo en las empresas, con dedicación exclusiva para el monitoreo y manejo de incidentes de seguridad, ya que al presentarse podrá resolverlo de manera efectiva y eficaz. Además, refleja la necesidad de capacitar y concientizar a todo el personal de la entidad ya que en la actualidad la mayoría de las personas cuentan con conexión a internet y podrían ser víctimas de ataques cibernéticos.

De igual forma, en el estado colombiano se presenta una debilidad en las políticas de seguridad informática. Lo anterior, por la falta de inversión en herramientas y personal capacitado en seguridad informática, tan solo en el año 2016, el presupuesto para la seguridad digital no llegó al 1% para la capacitación a los empleados y personal exclusivo en el área de seguridad digital.

[24] POLICIA NACIONAL y CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES, Óp. cit., p. 8.

También, se identificó que durante el año 2016 los tipos de incidentes más comunes fueron el *malware* y el *phishing*. En la Figura 1 se clasifica el aumento del *phishing* por sector en Colombia para el año 2016.

Figura 1. Aumento de *Phishing* por Sector 2016 en Colombia



Fuente: Autor con base en, Banco Interamericano de Desarrollo; Ministerio de Tecnologías de la Información y las Comunicaciones y Organización de los Estados Americanos. “Impacto de Los Incidentes de Seguridad Digital en Colombia 2017”. [En línea]. [Consultado: 19 de mayo de 2018]. Disponible en http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

Teniendo en cuenta el auge en los últimos cinco años de aplicaciones y plataformas que recaban información de los usuarios, la falta de conciencia de los consumidores digitales frente a la seguridad de su información y de acuerdo con las fuentes suministradas en el desarrollo de este acápite, se puede evidenciar, a partir de las cifras en informes oficiales internacionales y nacionales, que mediante la técnica del *phishing* se genera una afectación en la economía personal, empresarial y estatal, adicionalmente, se genera desconfianza en el uso de medios digitales en la sociedad, por lo tanto surgen las preguntas ¿Cuál ha sido el impacto del *phishing* en términos sociales y económicos en Colombia durante los últimos cinco años? Y ¿Cuáles estrategias de seguridad de la información se recomiendan para la mitigación del impacto del *phishing* en el país?

2. JUSTIFICACIÓN

El *phishing* como delito informático es practicado ampliamente hacia los usuarios de correo electrónico y redes sociales, debido a que, los cibercriminales usan formas sutiles de engañar a personas con poco conocimiento o descuido en actividades digitales, logrando así el robo de información, claves bancarias, influencia psicológica y estafas.

Esta práctica criminal ha tenido gran impacto a nivel mundial, regional y local; se estima que un porcentaje del 18% de los usuarios han sido víctimas de este delito en Estados Unidos, de la misma forma y de acuerdo con una encuesta realizada por ESET Latinoamérica[25], los servicios más suplantados por los cibercriminales a través del *phishing* son el web mail (correo electrónico en línea) con el 46%, redes sociales con un 45%, y bancos con el 44%. Tal como se observa en la Figura 2.

Figura 2. Encuesta ESET Latinoamérica

El Phishing Delito Informático

Pais	Usuarios Victimas
Estados Unidos	18%

Modalidades en Latinoamerica

Tipo	Usuarios Victimas
webmail	46%
Redes Sociales	45%
Bancos	44%

Fuente: Autor con base en, Goujon, André. *Phishing*: Webmail, Redes Sociales Y Bancos Son Los Servicios Más Suplantados. [en línea]. Welivesecurity, enero de 2013. [Consultado 12 de mayo de 2018]. Disponible en: https://www.welivesecurity.com/la-es/2013/01/09/*phishing*-webmail-redes-sociales-bancos-servicios-mas-suplantados

[25] Goujon, André. Phishing: Webmail, Redes Sociales Y Bancos Son Los Servicios Más Suplantados. [en línea]. Welivesecurity, enero de 2013. [Consultado 12 de mayo de 2018]. Disponible en: https://www.welivesecurity.com/la-es/2013/01/09/phishing-webmail-redes-sociales-bancos-servicios-mas-suplantados

El crecimiento de la tecnología trajo consigo uniformemente el crecimiento de los ataques informáticos y las nuevas modalidades de ciberdelitos, entre ellos, el *phishing* que ha tomado mayor fuerza durante los últimos años, ya que, tiene diferentes finalidades de uso de acuerdo con los objetivos de los ciberdelincuentes, afectando así, en diferentes niveles a todos los sectores en Colombia, por ello, es importante identificar cual es el impacto que genera la práctica de la técnica del *phishing* en Colombia, incluyendo sus diferentes modalidades y finalidades de uso.

Los ataques de *phishing* están dirigidos principalmente a los usuarios empresariales, debido a que, pueden obtenerse grandes ganancias con menores esfuerzos. La metodología usada para estos casos es el *spear-phisher.* "La diferencia entre los ataques de *phishing* común basado en email y el *spear-phishing* es que, no son ataques aleatorios y generalizados, sino que están dirigidos a una organización o individuo en particular"[26].

En el marco de este estudio monográfico se analiza información bibliográfica referente a los ciberdelitos, específicamente el *phishing* y su impacto en Colombia durante los últimos cinco años en términos sociales y económicos, identificando las causas más comunes, por las cuales, son vulnerables los sectores que presentan mayores denuncias por delitos informáticos en Colombia. El propósito es determinar cómo impacta el ataque de *phishing* y proponer cuáles pueden ser las mejores estrategias para la seguridad informática, con el fin de mitigar el *phishing* en Colombia.

[26] BELISARIO MÉNDEZ, Aymara Noriley. Análisis de Métodos de Ataques de Phishing. Buenos Aires, 2014, 61 páginas. Trabajo de grado (Especialista). Universidad de Buenos Aires. Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería. [Consultado 12 de mayo de 2018] [En línea] Disponible en http://bibliotecadigital.econ.uba.ar/?c=tpos&a=d&d=1502-0840_BelisarioMendezAN

3. OBJETIVOS

3.1 GENERAL

Proponer estrategias de seguridad de la información a través de controles y buenas prácticas para la mitigación del impacto de *phishing* en los sectores más atacados por este delito informático en Colombia durante los últimos cinco años.

3.2 ESPECÍFICOS:

- Clasificar las modalidades de *phishing* utilizadas en Colombia frente a la concurrencia y finalidad de uso de los ciberdelincuentes.
- Identificar el impacto económico y social del *phishing* en los sectores con mayores denuncias en Colombia durante los últimos cinco años.
- Establecer las vulnerabilidades más comunes de seguridad de la información en los sectores con mayores denuncias en Colombia durante los últimos cinco años.
- Identificar las estrategias y controles para la mitigación del *phishing* recomendadas en las políticas públicas relacionadas con la seguridad informática en Colombia.

4. DELIMITACIÓN

La presente monografía está basada en un estudio bibliográfico sobre el impacto de *phishing* en Colombia durante los últimos cinco años, periodo comprendido entre el año 2015 hasta el año 2019. Teniendo en cuenta que, en la actualidad existen nuevos métodos de *phishing*. En esta monografía solo se mencionarán los tipos más relevantes, los cuales se han venido presentando de forma continua en los últimos años, tales como: *phishing, vishing, smishing, whaling* o ataque BEC y *spear-phishing.*

De igual forma, se mencionan algunas herramientas generales utilizadas por los *phisher* para los ataques de *phishing*. Sin embargo, no se profundiza en ellas ya que esta monografía más que estar enfocada en la parte técnica, está dirigida a cualquier tipo de lector. Asimismo, aunque se toma como punto de referencia los sectores con más denuncias por ciberdelitos, la identificación de vulnerabilidades y estrategias propuestas de mitigación de *phishing* aplica para todos los sectores del país. Por lo tanto, no se realiza un análisis profundo en cada sector.

Por último, la propuesta sobre las estrategias, basadas en controles y buenas prácticas que pueden implementarse, para la mitigación de *phishing.* No son una política de seguridad de la información, ya que cada empresa tiene necesidades diferentes y específicas, sin embargo, las estrategias propuestas, sí pueden implementarse dentro de la política de seguridad de la información de una empresa.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

En este acápite, se muestran algunos estudios realizados anteriormente, sobre el tema de estudio; por lo tanto, se presentan conclusiones, relevantes y complementarias para esta monografía.

De acuerdo con el estudio realizado por Plazas[27], en el año 2018, se determinó que el usuario es el eslabón más débil a la hora de realizar un ataque de ingeniería social y que en los últimos años se han incrementado dichos ataques en las empresas colombianas ya que no invierten en herramientas seguridad informática, ni en las capacitaciones para los usuarios, por lo tanto, desconocen cómo deben actuar frente a un ataque de ingeniería social. Adicionalmente afirma que el sector bancario es el más afectado utilizando la técnica de *phishing*.

Rodríguez, en su estudio, muestra los diferentes actores y la afectación a las víctimas ante un ataque de *phishing* al concluir que: "ante un evento de *phishing* el banco es la víctima, no el consumidor financiero, ya que la pérdida se da sobre el patrimonio de aquél y no de éste, sin perjuicio de que el engaño que ha sufrido el banco y la automatización contable de la operación le lleva a inscribir en el registro del usuario la transacción de reembolso y que el ordenamiento jurídico colombiano ha asignado al banco el riesgo de pérdida frente a los eventos de *phishing*" [28].

Según Ruiz[29], en su monografía Diseño de Modelo de Seguridad Informática Basado en la Gestión de Incidentes para el área de Sistemas y Tecnología de Abril Publicidad en Bogotá Colombia, afirma que es importante incluir las áreas y usuarios que podrían afectar la seguridad de la información y complementa esta idea con

---

[27] PLAZAS GARCIA, Edna Roció. Ingeniería Social en las Empresas Colombianas. [En línea]. Pitalito, 2018, 75 Pág. Monografía. Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad Informática. [Consulado: 10 de noviembre de 2019]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

[28] RODRÍGUEZ PUENTES, Marcos. Responsabilidad bancaria frente al phishing. [En línea]. Bogotá, 2015,102 Pág. Monografía. Universidad Nacional de Colombia. Facultad de Derecho, Ciencias Políticas y Sociales. Departamento de Derecho. [Consulado: 10 de noviembre de 2019]. Recuperado de http://bdigital.unal.edu.co/53188/1/marcosrodriguezpuentes.2015.pdf

[29] RUIZ ALONSO, Luis Alejandro. Diseño de Modelo de Seguridad Informática Basado en la Gestión de Incidentes para el área de Sistemas y Tecnología de Abril Publicidad en Bogotá Colombia. [En línea]. Bogotá, 2014, 86 Pág. Monografía. Universidad Piloto de Colombia, Facultad de Posgrados, Especialización en Seguridad Informática. [Consulado: 10 de noviembre de 2019]. Recuperado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2976/00001518.pdf?sequence=1&isAllowed=y

que, capacitar y sensibilizar a todos los usuarios puede edificar un buen modelo de gestión de la seguridad de la información.

5.2 MARCO TEÓRICO

5.2.1 Seguridad Informática vs Seguridad de la información. Para Baca, “la seguridad informática es la disciplina que, con base en políticas y normas internas y externas de la empresa, se encarga de proteger la integridad y privacidad de la información que se encuentra almacenada en un sistema informático, contra cualquier tipo de amenazas, minimizando los riesgos tanto físicos como lógicos, a los que está expuesta”[30]. Complementando esta idea, Aguilera[31] explica que un sistema informático está constituido por un conjunto de elementos físicos, es decir el hardware, lo que es tangible de un equipo tecnológico; el software la parte lógica, lo que es intangible e inteligente del mismo y los elementos humanos siendo los que dan funcionamiento que requiere al hardware y al software.

Sin embargo, la seguridad informática generalmente es confundida con la seguridad de la información y aunque van de la mano, son diferentes. Según Pérez, “la seguridad de la información es la protección de la integridad, disponibilidad y confidencialidad de la información, según el nivel requerido para los objetivos de negocio de la empresa”[32]. Es decir que, la seguridad informática hace referencia a la protección de los sistemas informáticos (hardware, software, humanos), por tanto, la información almacenada en ellos y la seguridad de la información abarca toda la información incluyendo la que se encuentra por fuera de un sistema informático.

Es importante resaltar que la información es el activo más importante, entendiéndose como activo a cualquier pertenencia de la empresa que tiene valor para su funcionamiento. Por lo tanto, deben ser protegidos y cumplir con los pilares de la seguridad de la información, en su gran mayoría los autores mencionan tres: la disponibilidad, integridad y confidencialidad; sin embargo, se puede incluir la

---

[30] BACA URBINA, Gabriel. Introducción a la Seguridad Informática [en línea]. México: Grupo editorial Patria, 2016. 331 p. [Consultado: 11 de octubre de 2020]. Disponible en: https://books.google.com.co/books?id=IhUhDgAAQBAJ&printsec=frontcover&dq=seguridad+informatica&hl=es&sa=X&ved=2ahUKEwiJv-PVgazsAhWMxFkKHQGICbkQ6AEwAHoECAMQAg#v=onepage&q&f=true ISBN: 978-607-744-471-8

[31] AGUILERA, Purificación. Seguridad Informática [en línea]. Editex, 2010. 240 p. [Consultado: 11 de octubre de 2020]. Disponible en https://books.google.es/books?id=Mgvm3AYIT64C&dq=seguridad+inform%C3%A1tica&lr=lang_es&hl=es&source=gbs_navlinks_s

[32] Pérez, J. C. Protección de datos y seguridad de la información: guía práctica para ciudadanos y empresas (4a. ed.). [en línea]. RA-MA Editorial. 2015. 277 p. [Consultado: 11 de octubre de 2020]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/106483?page=1 ISBN: 9788499645919

trazabilidad y la autenticidad tal como se encuentran definidos en el libro de MAGERIT:

- Disponibilidad: o disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. La disponibilidad afecta directamente a la productividad de las organizaciones.

- Integridad: o mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

- Confidencialidad: o que la información llegue solamente a las personas autorizadas. Contra la confidencialidad o secreto pueden darse fugas y filtraciones de información, así como accesos no autorizados. La confidencialidad es una propiedad de difícil recuperación, pudiendo minar la confianza de los demás en la organización que no es diligente en el mantenimiento del secreto, y pudiendo suponer el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

A estas dimensiones canónicas de la seguridad se pueden añadir otras derivadas que nos acerquen a la percepción de los usuarios de los sistemas de información:

- Autenticidad: Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos. Contra la autenticidad de la información podemos tener manipulación del origen o el contenido de los datos. Contra la autenticidad de los usuarios de los servicios de acceso, podemos tener suplantación de identidad.

- Trazabilidad: Aseguramiento de que en todo momento se podrá determinar quién hizo qué y en qué momento. La trazabilidad es esencial para analizar los incidentes, perseguir a los atacantes y aprender de la experiencia. La trazabilidad se materializa en la integridad de los registros de actividad[33].

5.2.2 Delitos Informáticos. Como se mencionaba anteriormente, la información es el activo más importante de una empresa, esta información puede ser almacenada dentro o fuera de un sistema informático, por lo tanto, todo se debe proteger. Pero ¿De qué se debe proteger? De los ciber-ataques que tienen como fin dañar los sistemas informáticos, hurtar dinero, acceder de forma abusiva a información confidencial, entre otros. La policía cibernética lo define como “criminalidad

[33] MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. [en línea]. Madrid, Subdirección General de Información, Documentación y Publicaciones Jesús González Barroso, octubre de 2012. 127 p. [Consultado: 11 de octubre de 2020]. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html NIPO: 630-12-171-8

relacionada con el uso de las Tecnologías de la información y la Comunicación"[34]. En una encuesta realizada a 127 hackers la motivación principal de realizar ciberataques es la búsqueda de emociones[35]. Frente este aspecto, el Doctor Posada afirma que:

> los delitos informáticos vinculados a la red (pero que no dependen de la red), también llamados delitos computacionales *o informáticos en sentido amplio*, son todas aquellas conductas punibles tradicionales de medios ejecutivos abiertos, que tienen una relación modal objetiva -aunque circunstancial- con el tratamiento de datos e información y los sistemas informáticos (utilización de elementos incorporales). Son delitos que directamente lesionan o ponen en peligro bienes jurídicos como el patrimonio económico. La fe pública, la intimidad personal, la libertad y la formación sexual, el honor, los derechos morales y patrimoniales de autor[36].

Muestra de estas lesiones de los delitos informáticos, es la ejecución de uno de los ciberataques más fuertes de los últimos años, el virus tipo *ransomware* llamado *WannaCry*. Según la revista Semana afectó 74 países, entre ellos España, Taiwán, Rusia, Portugal, Ucrania, Turquía y Reino Unido, logrando colapsar el Servicio Nacional de Salud; se define en este artículo el *ransomware* como: "un ataque que tiene como metodología enviar correos con una modalidad llamada *Spear Phishing* en donde el ciberdelincuente adjunta un archivo atractivo para la víctima, cuando el usuario lo recibe y abre el archivo adjunto la información del disco duro del PC es cifrada, posteriormente el ciberdelincuente envía un mensaje en donde solicita una compensación económica para poder regresar la información"[37].

Además de solicitar el valor del rescate en bitcoin, que es una moneda virtual para desencriptar la información. No es garantía que se lleve a cabo el rescate de la información, ya que posiblemente, aunque se pague el dinero que el ciberdelincuente solicita, se puede perder la información totalmente y a medida que

---

[34] POLICIA NACIONAL. Amenazas del Cibercrimen en Colombia 2016-2017. [En línea]. [Consultado 5 de mayo de 2019]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

[35] PANDA. En la cabeza del cibercriminal: ¿qué busca y por qué quiere atacar tu empresa? 2015. [En línea]. [Consultado 5 de mayo de 2019]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/en-la-cabeza-del-cibercriminal-que-busca-y-por-que-quiere-atacar-tu-empresa/

[36] POSADA MAYA, Ricardo. Los cibercrímenes: Un nuevo paradigma de criminalidad. Un estudio del título VII bis del Código Penal colombiano. [en línea]. Bogotá: Grupo Editorial Ibáñez, 2017. 484 p. [Consultado: 11 de octubre de 2020]. Disponible en https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/118331?page=7 ISBN 9789587498141

[37] Ola de ataques informáticos en todo el mundo. En: *revista Semana.* [en línea]. Diciembre de 2017. [Consultado: 23 de octubre de 2018]. Disponible en: https://pruebas.semana.com/tecnologia/articulo/ola-de-ataques-informaticos-en-todo-el-mundo/524914

pasa el tiempo va aumentado el valor solicitado. Este es solo un ejemplo de un virus que ha generado grandes pérdidas y daños en diferentes países del mundo, ya que, existen muchos más como son los gusanos, *malware*, troyanos y diferentes tipos de programas maliciosos, así mismo, todo el tiempo existe el riesgo a estar expuestos a estos ciberataques.

Es por esto, por lo que diferentes países se han concientizado de la importancia de la seguridad informática y de la seguridad de la información, que es atentada por los delitos informáticos a través los diferentes tipos de ciberataques. Estos, están enfocados a gobiernos específicos, han llegado al punto de crear una ***ciberguerra*** a nivel mundial, que afecta la infraestructura crítica tecnológica y otras áreas; por medio de diferentes ataques como denegación de servicios, *ciberespionaje*, robo de información gubernamental, afectación en las páginas oficiales de los estados y bancos. Algunos ejemplos de los ataques más conocidos por su gran impacto se muestran en la Tabla 1:

Tabla 1. Ciberataques históricos

2011: DUQU	2012: FLAME	2012: OFENSIVA CIBEROPERACIÓN SHAMOON
llevada a cabo presuntamente por Estados Unidos junto con Israel. Fueron ciberoperaciones diseñada en la Administración de Presidente George W. Bush, a través de acciones desplegadas desde noviembre del 2005 a junio del 2012 a objetivos estratégicos en Irán Sobre Juegos Olímpicos, Duqu es un gusano tipo troyano que "recolecta [información de] inteligencia de diferentes blancos".	Flame es una sofisticada ciberarma, que incluso algunos expertos indican que es la "más grande y la de más alto funcionamiento jamás descubierta", la cual puede, de acuerdo con las instrucciones del controlador y con alta versatilidad, "robar datos y conversaciones de las redes sociales, tomar fotografías instantáneas desde el computador, penetrar a través de redes, activar el micrófono para grabar audio, y buscar los dispositivos bluetooth activos", así mismo puede "espiar programas de mensajería instantánea, a navegadores como Internet Explorer y Mozilla, o programas como Microsoft Office o Adobe Acrobat	Irán llevó a cabo durante el año 2012 diferentes ciberataques a sistemas de cómputo en países como Estados Unidos, Arabia Saudí y Qatar, que transcurrieron así: Enero del 2012: ataques de DDoS contra bancos en los Estados Unidos. Julio del 2012: ciberataques contra la Empresa de Petróleos de Arabia Saudita. Se desata un virus llamado "Shamoon" que destruye los datos de 30.000 computadores. Este virus también sobrescribió el "registro maestro de arranque" de los computadores afectados, y estaba diseñado para mostrar la "bandera de los Estados Unidos quemándose". Agosto del 2012: ataque cibernético que deshabilita los sitios web y el sistema de correos electrónicos en Rasgas, compañía de gas natural de Qatar. También se presentaron ataques a la compañía saudí Aramco, en la cual se destruyeron decenas de computadores. Septiembre del 2012: ciberataques contra bancos de Estados Unidos a través de denegación de servicio, afecta al hitBank of America Corp., J.P. Morgan Chase & Co., U.S. Bancorp, PNC Financial Services, y el Wells Fargo & Co. Octubre del 2012: otra oleada de ataques afectó el desempeño de los sitios web de algunos bancos, incluso algunos estuvieron temporalmente offline. Así mismo, en Israel la Bolsa de Tel Aviv y el sitio web de una compañía aérea israelí fueron atacados sufriendo interrupciones

Fuente: Autor, con base en SALAZAR, juan., n.d. Sites.oas.org [en línea]. [Consultado: 23 de agosto de 2019]. Disponible en: https://www.sites.oas.org/cyber/Documents/2016%20-%20La%20migracio%CC%81n%20de%20la%20guerra%20al%20espacio%20digital-Juan%20Pablo%20Salazar.pdf

5.2.3 Derecho Informático. Con el fin de hacerle frente a los delitos informáticos, nace el concepto del derecho informático, como una herramienta para penalizar dichos delitos. De acuerdo con la definición del centro de investigación de derecho informático de la Universidad Externado de Colombia, "es aquel conjunto de principios y normas que regulan los efectos jurídicos del manejo de la informática, teniendo en consideración su variación, tendencias, usos e implicaciones legales. De esta manera, el derecho informático es la materialización del derecho de la informática, dado que permite otorgar soluciones jurídicas a los problemas que surgen dentro del manejo de la información electrónica"[38].

Agrega que "es una nueva disciplina jurídica, que cuenta con un *nomen iuris*, un objeto de estudio propio e independiente, que surge a raíz de un fenómeno de orden global, que hoy por hoy se ha convertido en el mecanismo por excelencia para la transmisión de la información, la celebración de los diferentes negocios jurídicos y el manejo de relaciones sociales terciarias"[39].

Actualmente, el mundo viene en un rápido desarrollo digital y esto de alguna manera obliga a que los estados avancen tecnológicamente, y se hace necesario la implementación de nuevas leyes y políticas que protejan la información y las estructuras tecnológicas. De esta necesidad nace el convenio de BUDAPEST, que está compuesto por aproximadamente 66 países y busca armonizar la tipificación y penalización de los ciberdelitos, en la legalidad de cada país perteneciente al convenio. Desafortunadamente, aún existen varios países que hacen muy poco por la ciberseguridad y ciberdefensa de sus países. Colombia es uno de los países Latinoamericanos que más se ha tomado en serio la seguridad de información y de la informática, implementando políticas públicas enfocadas a la seguridad digital del país, creando nuevas leyes y haciendo parte del convenio de *BUDAPEST*.

5.2.4 Convenio Budapest. El convenio sobre la ciberdelincuencia se realizó el 23 de noviembre del 2001 en Budapest, nace de la necesidad de penalizar internacionalmente los ciberdelitos, ya que en cada país estos delitos son penalizados y tipificados de diferente manera o en casos peores no están ni tipificados ni penalizados. Por lo tanto, lo que logra el convenio internacional de Budapest es realizar la regulación armonizada de la tipificación y penalización de los ciberdelitos teniendo en cuenta los que son más semejantes y rompiendo las barreras territoriales, ayudando de esta manera a la detección, investigación y sanción de los ciberdelitos.

Es necesario aclarar que las sanciones penales se podrán realizar únicamente en los países que se han unido a este convenio, ya que desafortunadamente no han

[38] CENTRO DE INVESTIGACIÓN DE DERECHO INFORMÁTICO – CIDI. [en línea]. Universidad Externado de Colombia. [Consultado: 11 de octubre de 2020]. Disponible en: https://www.uexternado.edu.co/centro-investigacion-derecho-informatico-cidi/

[39] CENTRO DE INVESTIGACIÓN DE DERECHO INFORMÁTICO – CIDI. Objeto de Estudio, Óp. cit.

sido todos los países, por lo tanto, si un ciberdelincuente comete un delito informático en un país que no hace parte del acuerdo Budapest y si en ese país no existen leyes donde penalicen el delito informático, el ciberdelincuente quedara libre de toda culpa.

Está conformado por 46 artículos, divididos en cuatro capítulos, donde se define y clasifica los delitos como:

- Delitos que tienen a la tecnología como fin: son aquellos que atentan contra la confidencialidad, integridad o disponibilidad de la información. Por ejemplo, el daño informático, el acceso ilícito a un sistema, etc.

- Delitos que tienen a la tecnología como medio: se refiere a delitos ya conocidos, que se cometen a través de un sistema informático. Son delitos comunes, que ya se encuentran tipificados en la mayoría de las legislaciones, ampliados a los medios digitales. Por ejemplo, el fraude informático o la falsificación de datos digitales.

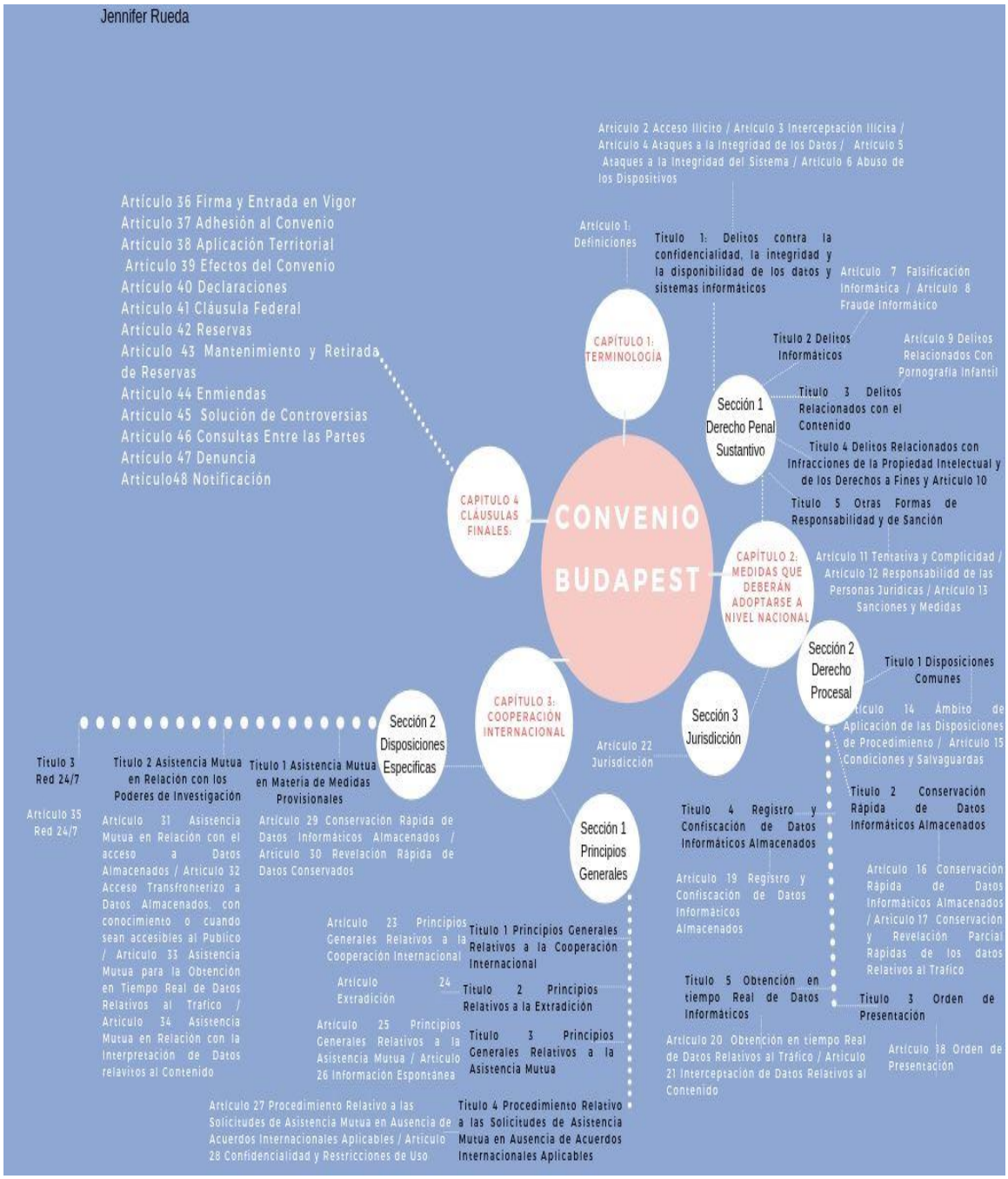
- Delitos relacionados con el contenido: establece como delitos diversos aspectos de la producción, posesión y distribución electrónica de pornografía infantil.

- Delitos relacionados con infracciones a la propiedad intelectual: se refiere a la reproducción y difusión en Internet de contenido protegido por derechos de autor, sin la debida autorización. Por ejemplo: infracciones a la propiedad intelectual, piratería, etc[40].

También abarca temas como las normas procesales, normas de cooperación internacional, entre otros. En Colombia en junio del 2018 el Congreso de la República aprobó la adhesión a este convenio, queriendo hacer parte de los más de 56 países que luchan contra la ciberdelincuencia por medio de este acuerdo, en la Figura 3 se muestra la estructura de manera general del Acuerdo de Budapest:

[40] PASTORINO, Cecilia. Convenio de Budapest: beneficios e implicaciones para la seguridad informática. [En línea]. WELIVESECURITY. Diciembre de 2017. [Consultado: 06 de diciembre de 2017]. Disponible en https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/

Figura 3. Convenio de Budapest



Fuente: Autor, con base en BUDAPEST. CONSEJO DE EUROPA, *et a*l. Serie de tratados europeos 185. (21, noviembre, 2001). Convenio sobre la ciberdelincuencia [en línea]. [Consultado: 20 de febrero de 2020]. Disponible en: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

5.2.5 CONPES 3701. En Colombia el 14 de Julio de 2011 el Consejo Nacional de Política Económica y Social – CONPES aprueba el documento llamado CONPES 3701: Lineamientos de Política para Ciberseguridad y Ciberdefensa, desarrollado con el apoyo de, el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Interior y Justicia, el Ministerio de Relaciones Exteriores, el Departamento Nacional de Planeación y el Departamento Administrativo de Seguridad.

Como su título lo menciona, el objetivo es crear lineamientos de políticas de prevención y control con el fin de contrarrestar las amenazas informáticas que afectan el País, ya que se identifican algunas debilidades para enfrentarlas, por lo tanto, es necesario el fortalecimiento de la capacidad del Estado para hacerle frente a dichas amenazas. Este documento cuenta los antecedentes nacionales e internacionales en cuanto a algunos ataques informáticos, la normatividad y políticas que se han ido desarrollando para la ciberseguridad y ciberdefensa, e iniciativas de entidades tanto a nivel público como privado que buscan una mejora continua en la seguridad informática. Presenta un diagnóstico sobre la problemática, mostrando el problema central y los efectos sobre el mismo, identificando tres ejes problemáticos:

1. Las iniciativas y operaciones en Ciberseguridad y Ciberdefensa no están coordinadas adecuadamente.

2. Debilidad en la oferta y cobertura de capacitación especializada en Ciberseguridad y Ciberdefensa.

3. Debilidad en regulación y legislación de la protección de la información y de los datos.

Ante estas problemáticas, se establece un objetivo central y, como solución a las tres problemáticas mencionadas anteriormente se definen tres objetivos específicos:

1) “Implementar instancias apropiadas para prevenir, atender, controlar y generar recomendaciones que regulen los incidentes y/o emergencias cibernéticas para proteger la infraestructura crítica nacional.

2) Diseñar y ejecutar planes de capacitación especializada en ciberseguridad y ciberdefensa.

3) Fortalecer el cuerpo normativo y de cumplimiento en la materia”[41].

[41] COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, *et al*. CONPES 3701. (14, julio, 2011). Lineamientos de Política para Ciberseguridad y Ciberdefensa. [en línea]. [Consultado: 12 de mayo de 2019]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

Igualmente, el documento muestra un plan de acción para implementar las propuestas definidas en los objetivos, donde se propone en relación con el primer objetivo la creación de:

- ColCERT: El Grupo de Respuesta a Emergencias Cibernéticas de Colombia - colCERT, tiene como responsabilidad central la coordinación de la Ciberseguridad y Ciberdefensa Nacional, la cual estará enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal será la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional[42].

- Centro Cibernético Policial - CCP Estará encargado de la ciberseguridad del territorio colombiano, ofreciendo información, apoyo y protección ante los delitos cibernéticos. Desarrollará labores de prevención, atención, investigación y judicialización de los delitos informáticos en el país, informando en su página web sobre vulnerabilidades cibernéticas. Recibirá y atenderá los lineamientos nacionales en ciberseguridad y trabajará de forma coordinada con el colCERT.

- El Comando Conjunto Cibernético (CCOC) planea, coordina, integra y conduce operaciones militares en el ciberespacio para la defensa de los intereses nacionales y de la infraestructura crítica cibernética nacional a fin de contribuir en el cumplimiento de la misión del Comando General de las Fuerzas Militares[43].

En relación con el segundo objetivo, capacitaciones para los funcionarios directamente involucrados, como por ejemplo el personal que hace parte de las instituciones que conformarían el colCERT, CCP y CCOC; la policía judicial y otros donde se incluye el SENA y la Fiscalía General de la Nación, como capacitadores y el colCERT para crear programas de sensibilización y concienciación para los ciudadanos en general. También se busca en este segundo objetivo, identificar la infraestructura crítica en Colombia.

Y en relación con el tercer objetivo se propone una reforma a las leyes actuales y si es el caso la creación de nueva normatividad y legislación con el fin de mejorar los procesos de prevención, investigación y judicialización de los ciberdelitos favoreciendo la ciberseguridad y ciberdefensa en Colombia, ya que aún existen grandes vacíos jurídicos para la penalización de estos delitos. También como

[42] Grupo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT. Acerca de. [En línea]. Julio de 2017. [Consultado: 12 de julio de 2018]. Disponible en http://www.colcert.gov.co/?q=acerca-de

[43] COMANDO CONJUNTO CIBERNÉTICO. Misión y Responsabilidad. [En línea]. [Consultado: 21 de noviembre de 2017]. Disponible en https://www.ccoc.mil.co/quienes_somos/mision_responsabilidad

camino de mejora busca la cooperación internacional donde se realiza la solicitud de adherirse a convenios internacionales como el convenio de Budapest.

Adicionalmente, este documento especifica el financiamiento requerido para la implementación de las propuestas, dando los valores por año, del 2011 al 2014, en el Capítulo VII se encuentran las recomendaciones que reafirman de manera concreta las problemáticas y soluciones descritas anterior y finalmente, en el Capítulo VIII, se registran las fuentes bibliográficas.

Se considera que este documento tiene una gran importancia para el país en cuanto al avance de la concientización de las entidades públicas y privadas, sobre la importancia de implementar políticas públicas para la seguridad informática. Ya que, al tener conciencia de la importancia, de las grandes consecuencias de los ataques informáticos, permite visualizar las debilidades del estado, ante esta posible situación e inicia una propuesta con soluciones que son totalmente necesarias y que contribuye con el desarrollo y mejora continua de la ciberseguridad y ciberdefensa en Colombia.

5.2.6 CONPES 3854. En Colombia el 11 de abril de 2016 el Consejo Nacional de Política Económica y Social – CONPES aprueba el documento llamado CONPES 3854: Política Nacional de Seguridad Digital, desarrollado con el apoyo de, el Ministerio de Defensa Nacional, el Ministerio de Tecnologías de la Información y las Comunicaciones, Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación.

En este CONPES 3854 se identifica el crecimiento alarmante de conectividad en la red de los usuarios colombianos en redes sociales y diferentes servicios en línea, a medida que incrementa la tecnología. Es por esto, por lo que se hace necesario este documento para reforzar los objetivos del CONPES 3701 pero dando un enfoque a la gestión de incidentes. Fortaleciendo las entidades creadas como el colCERT, CCP Y CCOC, por medio de la educación; realizando una actualización periódica de la infraestructura critica en Colombia; y diseñando un modelo de gestión de riesgos de seguridad digital a nivel nacional.

En los *antecedentes normativos y política pública*: se hace referencia a los objetivos logrados en el CONPES 3701, según el Departamento Nacional de Planeación, en su seguimiento, cumplió con un 79%, con corte al informe de junio de 2015. Estos logros se clasifican más específicamente, de la siguiente manera:

- **Institucionalidad:** Se logran los objetivos planteados en cuanto al fortalecimiento de la institucionalidad mediante la creación de diferentes entidades o grupos de respuesta como el ColCERT del Ministerio de Defensa, el CCOC de las Fuerzas Militares, el CCP – Centro Cibernético de la Policía Nacional, el CSIRT PONAL – Equipo de Respuesta a Incidentes de Seguridad Informática de la Policía

Nacional. Así como también la Delegatura de Protección de Datos en la Superintendencia de Industria y Comercio, la Subdirección Técnica de Seguridad y Privacidad de Tecnologías de Información del MINTIC y el Comité de Ciberdefensa de las Fuerzas Militares y las Unidades Cibernéticas del Ejercito Nacional, la Armada Nacional y la Fuerza Aérea Colombiana. Adicionalmente la Comisión Nacional Digital y de Información Estatal mediante Decreto 32 de 2013 del MINTIC.

- **Capacitación:** En cuanto a las capacitaciones llevadas a buen término se destacan las campañas de sensibilización para uso responsable del internet enfocado a los niños y adolescentes, la formación especializada a servidores públicos. Asimismo, el colCERT capacitó a funcionarios del estado y del sector privado. También programas de sensibilización y concientización para la ciudadanía en general sobre ciberseguridad y ciberdefensa y el CCOC fortaleció las capacidades propias sobre ciberdefensa y capacito las unidades cibernéticas. Aplico lineamientos y directrices al interior de las instituciones. También el CCP realizo campañas de sensibilización a la ciudadanía en general sobre ciberseguridad y Acciones para fortalecer la investigación y judaización de delitos cibernéticos y se logró un avance significativo de ofertas académicas Especializadas, entre ellas certificaciones de reconocimiento Internacional.

- **Legislación:** El país desarrollo y aprobó normas, tales como la protección de datos personales, la regulación sobre protección contra, la pornografía, turismo sexual y demás formas de abuso sexual a menores de edad. También la protección a los derechos fundamentales establecido en la Ley 1581 de 2012 donde menciona temas como el reconocimiento de los datos e información como bien jurídico tutelado.

- **Cooperación Internacional:** Frente a las actividades de cooperación internacional, se menciona que, en 2013 a través del Ministerio de Relaciones Exteriores, el país solicita formalmente adherirse al convenio de BUDAPEST, el convenio multilateral con el foro económico mundial para identificar y abordar los riesgos sistemáticos globales derivados de la conectividad, además de que Colombia hace parte de una red de alerta que proporciona formación técnica a personal Especializado. Informa sobre los acuerdos con las organizaciones Internacionales como el Antipshing Working Group, así como también la Policía Nacional a través del CCP, sostiene mecanismos de cooperación con homólogos en otros países y agencias de Ley como: INTERPOL, FBI, EC3, AMERIPOL, KOLCA, NCA, INTERPOL (GLDTA) y ATA y que Colombia cuenta con ocho CSIRT – FIRST, asimismo que el CCOC elabora el catálogo de Infraestructura Critica Cibernética Nacional en Coordinación con las partes interesadas.

De acuerdo con la **Revisión y evaluación de los lineamientos de política,** se determinó que el Documento CONPES 3701 no puede interpretarse como una capacidad suficiente, integral y efectiva de preparación ante ataques cibernéticos

debido al constante crecimiento y sofisticación de los nuevos ciberataques. Ante esta situación el presidente de aquel momento Juan Manuel Santos, solicita la creación de una comisión de alto nivel y se crean mesas de trabajo durante el año 2014 y 2015, estas mesas de trabajo están compuestas por las nuevas organizaciones creadas en el CONPES 3701, es decir, el colCERT, CCP y CCOC. También con el apoyo de la OEA y expertos internacionales de otros gobiernos, algunas organizaciones y la INTRPOL.

La mesa de expertos Nacionales en esta revisión de la política la orientan a cinco dimensiones, la primera de ellas es la gobernabilidad y coordinación efectiva, seguido de la preparación y prevención, como tercera dimensión se encuentra el conocimiento de la situación actual, además la resiliencia, recuperación y respuesta, como última dimensión la efectiva cooperación e intercambio de información.

Por otra parte, la mesa de expertos internacionales de la OEA realizó una serie de recomendaciones, entre ellas desarrollar una visión estratégica global para la ciberseguridad, adoptar un enfoque nacional de la gestión de riesgos, establecer un marco institucional claro, asimismo, establecer un proceso sistemático para involucrar a todos los interesados en el desarrollo de la estrategia y su implementación y adoptar una estrategia para la protección y defensa de las infraestructuras críticas cibernéticas nacionales, siendo conscientes de la necesidad de fortalecer las capacidades operativas, administrativas, humanas, científicas, tecnológicas y de infraestructura física de las instituciones.

Finalmente, la mesa nacional y la internacional concluyen que debe implementarse nuevos elementos a las estructuras institucionales, a la legislación, acciones existentes y en la política, los lineamientos, principios, directrices relacionados con los derechos humanos en el entorno digital.

Luego se realiza un análisis sobre las **mejores prácticas internacionales**, y es de allí donde nacen los conceptos de gestión del riesgo, múltiples partes interesadas y responsabilidad compartida. Ya que, en los gobiernos con más avances en la implementación de seguridad digital, están enfocadas en ello. El siguiente párrafo es un pequeño resumen de ello:

Por su parte, el Consejo mundial de la industria de tecnologías de la información (ITI por sus siglas en inglés) expone que, para lograr un enfoque de múltiples partes interesadas y responsabilidad compartida, los gobiernos deben orientar sus estrategias a la gestión de riesgos, pero también a la concientización, sensibilización y educación. Los gobiernos deben buscar que todas las partes interesadas sean conscientes de su papel con el fin de hacer frente a los riesgos de seguridad digital. El ITI resalta que los esfuerzos deben incluir la sensibilización, a través de los sistemas educativos, a los ciudadanos de todas las edades sobre la seguridad digital, y que las múltiples partes interesadas necesitan saber cómo afrontar las incertidumbres y reducir los riesgos.

Esta sección termina mencionando de manera general, el marco normativo nacional e internacional sobre la ciberseguridad y dando como conclusión la necesidad de plantear una nueva política nacional de seguridad digital en Colombia.

En el *marco conceptual* expone los conceptos básicos sobre la seguridad digital, como riesgo, riesgo de seguridad digital, gestión de riesgo, entre otros. Y las características generales que debe tener una estrategia de gestión de riesgos de seguridad digital según las mejores prácticas internacionales; y con base en lo anterior establece los principios y dimensiones estratégicas que definen la política nacional de seguridad digital en el país.

La problemática o diagnóstico, menciona nuevamente el gran incremento de conectividad a internet de los colombianos en los últimos años y así mismo las afectaciones por incidentes de seguridad en la que se han visto afectados mayormente los ciudadanos, debido a la sofisticación de nuevos ciberataques. Con base en este diagnóstico nace la necesidad de implementar una política enfocada a la gestión de riesgos, para controlar los incidentes de seguridad, basados en las mejores prácticas internacionales.

> Su implementación atenderá cinco problemas principales: (i) no se cuenta con una visión estratégica en seguridad digital basada en la gestión de riesgos; (ii) las múltiples partes interesadas no maximizan sus oportunidades al desarrollar actividades socioeconómicas en el entorno digital; (iii) se necesita reforzar las capacidades de ciberseguridad con un enfoque de gestión de riesgos de seguridad digital; (iv) se necesita reforzar las capacidades de ciberdefensa con un enfoque de gestión de riesgos de seguridad digital; y (v) los esfuerzos de cooperación, colaboración y asistencia, nacional e internacional, relacionados con la seguridad digital no son suficientes y requieren ser articulados[44].

Se identifica que, la falta de coordinación nacional de seguridad digital, entre las diferentes instituciones, causa un desgaste en recursos y duplicación de esfuerzos ya que pueden presentarse situaciones tales como, por ejemplo, invertir en capacitaciones del mismo tema a los mismos usuarios. El BID y la OEA en el año 2016, reconoce el trabajo de Colombia en la creación del colCERT como grupo de respuesta de incidentes nacionales, sin embargo, lo clasifica como “formativo” ya que se encuentra limitado en cuanto a la detección y respuesta de incidentes, debido a esta falta de coordinación y a la dependencia de información externa. Por otra parte, Colombia enfoca sus esfuerzos en contrarrestar las amenazas cibernéticas que atenten contra la defensa y seguridad nacional, sin prestar mayor

---

[44] COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, *et al*. CONPES 3854. (11, abril, 2016). Política Nacional de Seguridad Digital. [en línea]. [Consultado: 21 de agosto de 2019]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

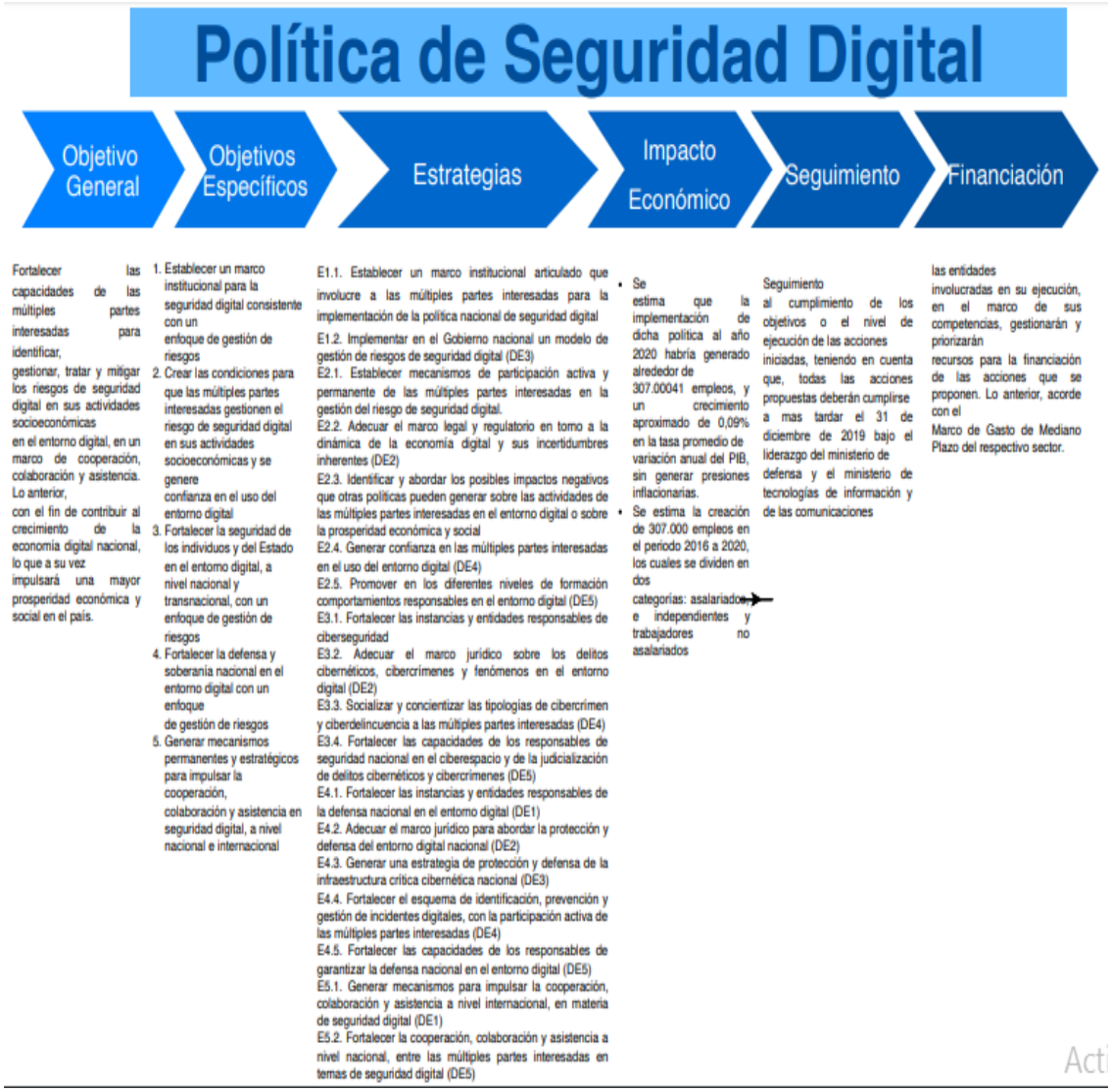
atención a maximizar las oportunidades del entorno digital en el sector privado y esto dificulta el crecimiento de la economía digital del país. Según estadísticas mencionadas en el CONPES, es la desconfianza por parte de las empresas y del consumidor a el entorno digital lo que ha impedido la inclusión a este medio.

De acuerdo con las cifras del Centro Cibernético Policial (CCP), el tipo, número de amenazas cibernéticas, denuncias y capturas entre 2014 y 2015 aumentaron notablemente y frente a las entidades del estado se da a conocer una gran brecha tecnológica y así como, su poca inversión en recursos tecnológicos y humanos para la seguridad digital, afectando de esta manera la justicia colombiana ya que los fiscales y jueces no cuentan con el conocimiento suficiente para sancionar este tipo de delitos. Por lo tanto, es necesario reforzar las capacidades de ciberseguridad con un enfoque de gestión de riesgos tanto en el sector público, como en el privado. Adicionalmente, recomienda la creación de nuevos CSIRT sectoriales, teniendo en cuenta los nuevos avances en los ciberataques, incluyendo los ataques a la infraestructura crítica ya que este es usado para infundir ciberterrorismo. Así mismo, se recomienda crear canales de comunicación donde se intercambie información entre el sector público y privado, incluyendo así todas las partes interesadas, con el fin de prevenir, detectar y contener nuevos ciberataques.

En el punto cinco, de este CONPES, se desarrolla la política de seguridad digital y dentro de las estrategias a implementar se destaca, la creación de un cargo como “Coordinador Nacional de Seguridad Digital”, el cual, con el apoyo de un equipo operativo intersectorial, como la Comisión Nacional Digital y de información estatal busca garantizar, la articulación entre las múltiples partes interesadas, con el fin de implementar un modelo de gestión de riesgos que permita prevenir, detectar y solucionar de manera eficiente y eficaz los incidentes de seguridad. También la creación de los cSIRT sectoriales, esto tendría entre otros beneficios, ganar la confianza en el sector público y privado sobre el uso de los medios digitales, obteniendo un crecimiento en la economía digital. Armonizar la institucionalidad con un nuevo enfoque de seguridad digital, daría solución a el desgaste en recursos y duplicación de esfuerzos de las diferentes instituciones.

Otras estrategias relevantes son, el fortalecimiento del colCERT como punto focal nacional para la gestión de incidentes; las capacitaciones por la plataforma de Colombia Aprende; la creación de un catálogo de infraestructura crítica cibernética nacional; y estrategia de protección y defensa. En la Figura 4 se muestra la estructura general de la política de seguridad digital.

Figura 4. Política Nacional de Seguridad Digital



Fuente: Autor, con base en, COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, *et al*. CONPES 3854. (11, abril, 2016). Política Nacional de Seguridad Digital. [en línea]. [Consultado: 21 de agosto de 2019]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

Finalmente, termina con recomendaciones realizadas por, el Ministerio de Tecnologías de la Información y las Comunicaciones, el Ministerio de Defensa Nacional, el Departamento Administrativo de la Presidencia, el Ministerio de Educación Nacional, el Ministerio del Interior, el Ministerio de Justicia y del Derecho,

el Ministerio de Relaciones Exteriores, el Departamento Administrativo Dirección Nacional de Inteligencia y el Departamento Nacional de Planeación. Cada recomendación está enfocada a realizar diferentes actividades de la mano con el coordinador Nacional de Seguridad Digital, para cumplir los objetivos establecidos.

5.2.7 Ingeniería Social. Las entidades públicas, privadas y la sociedad en general, se ven afectadas por los ataques informáticos, ya que estos buscan capturar información confidencial para lucrarse ilegalmente. Esto conlleva a grandes pérdidas económicas y daños sociales. No es posible establecer el número de ataques informáticos que existen hoy en día, ya que, continuamente desarrollan nuevas técnicas y vías de ataque. Sin embargo, una de las técnicas de ataque más utilizada es la ingeniería social por su gran facilidad y efectividad.

En una presentación de *The Open Web Application Security Project – OWASP se* define la ingeniería social como el "conjunto de técnicas psicológicas y habilidades sociales (tales como: la influencia, la persuasión y la sugestión). Busca directa o indirectamente que un usuario revele información sensible, sin estar conscientes de los riesgos que esto implica, b|1321Qasada en computadoras (*phishing*) y contacto humano (presencial, telefónico)"[45]. También establece que los puntos clave para llevar a cabo la ingeniería social son la psicología y la interacción social y que sus ataques se componen por 4 categorías, técnicos, ego, simpatía e intimidación. Los seres humanos son muy dados a entregar información confidencial sin notarlo, por ejemplo, al conocer nuevas personas por medios virtuales o presencialmente, de hecho, la cultura colombiana tiene esa tendencia de ser muy sociable y confiada, por lo tanto, entregan datos importantes con facilidad.

5.2.8 *Phishing.* Como se mencionó anteriormente el *phishing* es un ataque informático que se deriva de la ingeniería social. La palabra *phishing* nace de la similitud con *fishing,* que significa pescar y de eso se trata esta técnica, de pescar a una víctima que caiga en el engaño y entregue o acceda sin darse cuenta a lo que el *phisher* requiere, por lo tanto, es muy utilizada por los ciberdelincuentes ya que, al utilizar esta técnica, se ahorran bastante trabajo, teniendo solo que manipular y engañar al eslabón más débil, que es el usuario. Consiste en engañar al usuario para robar información de identidad y datos confidenciales como usuarios y contraseñas, números de cuentas, tarjetas de crédito, utilizando el envió de correos electrónicos con links de formularios y páginas web falsas, que hace creer a la víctima que la página suplantada es la página original. En la mayoría de los casos usan las páginas de portales bancarios, solicitando actualizar datos o prometen algún empleo, aprovechando la crisis laboral que existe en Colombia, además, les

[45] The Open Web Application Security Project – OWASP. Ingeniería Social. [en línea]. República Dominicana. OWASP LatamTour, 2016. [Consultado 12 de octubre de 2020]. Disponible en: https://owasp.org/www-pdf-archive/02_INGENIER%C3%8DA_SOCIAL.pdf

resulta muy efectivo, a raíz de esto el *phishing* ha aumentado en los últimos años y han mejorado y diseñado nuevas modalidades. La compañía *anti-malware Malwarebytes*, define el phishing como:

> Delito de engañar a las personas para que compartan información confidencial como contraseñas y números de tarjetas de crédito. Como ocurre en la pesca, existe más de una forma de atrapar a una víctima, pero hay una táctica de phishing que es la más común. Las víctimas reciben un mensaje de correo electrónico o un mensaje de texto que imita (o "suplanta su identidad") a una persona u organización de confianza, como un compañero de trabajo, un banco o una oficina gubernamental. Cuando la víctima abre el correo electrónico o el mensaje de texto, encuentra un mensaje pensado para asustarle, con la intención de debilitar su buen juicio al infundirle miedo. El mensaje exige que la víctima vaya a un sitio web y actúe de inmediato o tendrá que afrontar alguna consecuencia.
>
> Si un usuario pica el anzuelo y hace clic en el enlace, se le envía a un sitio web que es una imitación del legítimo. A partir de aquí, se le pide que se registre con sus credenciales de nombre de usuario y contraseña. Si es lo suficientemente ingenuo y lo hace, la información de inicio de sesión llega al atacante, que la utiliza para robar identidades, saquear cuentas bancarias, y vender información personal en el mercado negro[46].

Ante la gran facilidad y eficacia de esta técnica preferida por los ciberdelincuentes, se han creado varias modalidades de *phishing*, algunas son, el *vishing, smishing, spear-phishing, whaling o* ataque *BEC, phishing nigeriano, phishing* de clonación*, Tabnabbing.* En la Figura 5, se realiza un análisis sencillo de la tendencia de los ataques de *phishing* al sector financiero en 2017, con base en un informe presentado por kaspersky.

[46] MALWAREBYTES. Suplantación de identidad: (phishing). [en línea]. [Consultado: 10 de octubre de 2020] Disponible en https://es.malwarebytes.com/phishing/#:~:text=Suplantaci%C3%B3n%20de%20identidad%20(phishing),correo%20electr%C3%B3nico%20o%20llamada%20telef%C3%B3nica.

Figura 5. Informe Financiero Kaspersky

Fraudes Electrónicos
Año 2017

Incrementos

Concepto	Indicador %	Tendencia
Phishing Financiero	47,5%	↑
Usuarios MAC	56%	↑

Sistema Financerio

Concepto	Indicador %
Sistemas de Pago	16%
Tienda en Linea	11%

Fuente: Autor con base en: SECURELIST. Ciberamenazas financieras en 2017. [En línea]. Kaspersky. (28 de febrero de 2018). [Consultado: 15 de noviembre de 2018]. Disponible en: https://securelist.lat/financial-cyberthreats-in-2017/86317/

5.2.8.1 Fases Del *Phishing.* Para llevarse a buen término este ataque informático, el ciberdelincuente debe establecer unas fases para realizar su cometido, estas fases son relativas, dependiendo la modalidad y la herramienta que el delincuente informático desee utilizar. Sin embargo, en el artículo llamado, caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura; unifica las fases más mencionadas por diferentes autores, las cuales son:

- Planificación y configuración: en esta etapa se identifica la organización, individuo o un país entero. El objetivo principal es extraer detalles esenciales sobre la víctima y la red, para lo cual se puede hacer un análisis de tráfico. Posterior a este reconocimiento, se configuran los ataques mediante el despliegue de medios viables como el sitio web, correos electrónicos que contienen enlaces maliciosos, etc. Estas herramientas fundamentalmente redirigen a la víctima hacia una página web fraudulenta.

- Ataque de Phishing: esta es la segunda fase del ciclo donde tiene lugar la actividad real. Los atacantes envían correos electrónicos falsificados a la víctima, usando direcciones de correo electrónico recolectadas, que solicitan información confidencial a la víctima. Generalmente los emails de *Phishing*, se disfrazan de alguna página de una organización bancaria de buena reputación, que necesita la información personal de la víctima para actualizar sus registros, e indica a la víctima que debe responder urgentemente haciendo clic en algún enlace malicioso.

- Ruptura/Infiltración: en esta fase, la víctima hace clic en el enlace malicioso y, en cuanto lo hace, un malware se instala automáticamente en su dispositivo, lo que

permite al atacante acceder al sistema y comprometerlo, cambiar sus configuraciones y derechos de acceso. En algunos casos, hacer clic en el enlace malicioso, también puede dar lugar a que el usuario común sea re direccionado a alguna página falsa.

- Recopilación de datos: una vez que los atacantes acceden al sistema de la víctima, extraen los datos requeridos. Por ejemplo, si la víctima proporciona datos confidenciales de una cuenta bancaria, el atacante puede acceder a ella, lo que eventualmente puede conducir a pérdidas financieras para la víctima. En el caso de ataques de *malware*, los atacantes obtienen acceso remoto al sistema de la víctima y extraen los datos requeridos o realizan cualquier cambio según su voluntad. En casos más graves, los sistemas comprometidos pueden utilizarse para ataques de denegación de servicio (DOS).

- Extracción: esta es la fase final del ciclo. Después de obtener el acceso y la información requerida, se elimina toda la evidencia como las cuentas falsas del sitio web. Finalmente, se evalúa el grado de éxito de su ataque, para afinar sus futuros ataques[47].

5.2.8.2 Herramientas de *Phishing*. Existe una gran cantidad de herramientas y formas de llevar a cabo un ataque de *phishing* y estas varían de acuerdo con la modalidad de *phishing* que el delincuente informático quiera realizar y su objetivo final, ya que, puede ir dirigido a una persona, a una empresa, a servidores. etc. A continuación, se mencionan algunas:

- Kali Linux: "Es un proyecto de código abierto mantenido y financiado por *Offensive Security*, un proveedor de servicios de prueba de penetración y capacitación en seguridad de la información de clase mundial. Además de Kali Linux, *Offensive Security* también mantiene la base de datos de exploits y el curso en línea gratuito *Metasploit Unleashed*"[48]. Esta distribución basada en Debian GNU/Linux cuenta con un gran número de herramientas para realizar ataques de *phishing* y de otras categorías, unas de las más conocidas son Matelgo y Social Engineer Toolkit (SET) es una de las herramientas para realizar ataques dirigidos (spear-phishing) a personas u organizaciones. Hace parte del kit integrado de Kali Linux. Generalmente cuando se llevan a cabo estos ataques, se crean máquinas virtuales para conservar el anonimato.

- Clonación de páginas: Más que una herramienta es un método de realizar la suplantación de una página, ya que, consiste a grandes rasgos en copiar el código

[47] BENAVIDES, Eduardo, et al. Caracterización de Los Ataques de Phishing y Técnicas Para Mitigarlos. Ataques: Una Revisión Sistemática de La Literatura. [en línea]. Ciencia y Tecnología (1390-4051), vol. 13, no. 1, Jan. 2020, pp. 97–104. EBSCOhost, doi:10.18779/cyt.v13i1.357. [Consultado: 12 de octubre de 2020]. Disponible en: http://eds.b.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=1&sid=32b1d2c6-682a-4c86-86c7-c2fd65dc19ca%40pdc-v-sessmgr02

[48] KALI. Acerca de Kali Linux. [en línea]. [Consultado 12 de octubre de 2020]. Disponible en: https://www.kali.org/about-us/

fuente de una página original, modificar algunos códigos, crear unos scripts y cargarlos a un hosting gratuito y con unos pasos a seguir, ya está la página clonada lista para capturar datos como usuario y contraseña.

- VozIP: "Por lo general, el estafador crea un sistema de voz automatizado para hacer llamadas a personas y pedirles información privada. Para simular que la llamada procede de una entidad financiera, hacen uso de una Voz IP o voz automatizada que resulta verosímil por su similitud a las utilizadas por los bancos"[49]. Esta herramienta es utilizada específicamente para realizar la modalidad de vishing.

5.2.9 Casos de *Phishing* en Colombia. Uno de los casos más conocidos en Colombia, fue el de Juan Solano conocido como, "El rey de las Millas". Un phisher experto, de 26 años, que utilizando las técnicas de phishing y vishing, logró viajar por diferentes partes del mundo, con las millas acumuladas de varios famosos colombianos. Según la información del Centro Policial Cibernético la millonaria defraudación fue de $541,412,000 y describe los hechos como: "…ingresaba a través de la página life miles y hurtaba los datos personales de los diferentes viajeros mediante la utilización de programas como Phishing (suplantación de sitios web) y *Vishing* (Protocolo Voz sobre IP (VoIP) y de ingeniería social, de esta manera, engañaba personas para obtener información personal), en ocasiones personalidades de la farándula nacional, ya que vulneraba el sistema de seguridad de dicha plataforma para usarlos en su beneficio"[50].

"Un caso a resaltar fue el ocurrido durante el primer semestre de 2011, cuando el grupo "hacktivista" autodenominado Anonymous atacó a los portales de la Presidencia de la República, el Senado de la República, Gobierno en Línea y de los Ministerios del Interior y Justicia, Cultura y Defensa, dejando fuera de servicio sus páginas web por varias horas. Este ataque se dio en protesta al Proyecto de Ley por el cual se regula la responsabilidad por las infracciones al derecho de autor y los derechos conexos en Internet"[51].

En el año 2019 según un artículo publicado por ESET[52], un banco en Colombia fue víctima de suplantación por modalidad de *phishing*, este fue un ataque sofisticado

[49] CARDOZO, Rossana. Atención al 'vishing': cómo detectarlo y protegerse. [en línea]. BBVA, 30 de agosto de 2019. [Consultado: 12 de octubre de 2020]. Disponible en: https://www.bbva.com/es/py/atencion-al-vishing-como-detectarlo-y-protegerse/

[50] CENTRO CIBERNÉTICO POLICIAL: Capturado el "Rey de las millas [en línea]. [Consultado: 02 de julio de 2020] Disponible en: https://caivirtual.policia.gov.co/ciberseguridad/casos-operativos/capturado-el-rey-de-las-millas

[51] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3701. Óp. cit., p. 9.

[52] LUBECK, Luis. Phishing suplanta identidad de reconocido banco de Colombia y busca robar información financiera. En: Welivesecurity: Campaña de phishing activa dirigida a usuarios de Colombia suplanta identidad de reconocido banco con el objetivo de robar credenciales de acceso y datos de las tarjetas de crédito y débito [en línea] Junio, 2019. [Consultado: 14/08/2020]. Disponible en https://www.welivesecurity.com/la-es/2019/06/05/phishing-activo-reconocido-banco-colombia/

ya que incluso contaba con certificado SSL. Enviaban correos a los usuarios, indicando que se habían bloqueado todos los canales de acceso y que, por seguridad, ahora debían ser restablecidos, cuando los usuarios ingresaban al enlace, se dirigían a la página clonada y allí capturaban usuario y contraseña.

En septiembre del año 2016, la Registraduría Nacional informó que fue víctima de un ataque informático, por lo tanto, cuando los usuarios realizaban la consulta en la página para confirmar si eran jurados o querían conocer el puesto de votación, se mostraba una ventana emergente informándoles que la cédula consultada había sido retirada porque la persona había fallecido.

Aunque el ataque afecto la credibilidad en las votaciones del plebiscito, algunos partidos políticos se manifestaron por la desconfianza que generó, afortunadamente el ataque no tuvo consecuencias más grandes. Pero los ciberdelincuentes pudieron incrementar su ego.

5.3 MARCO CONCEPTUAL

Se presenta a continuación el conjunto de conceptos necesarios, definiendo de manera específica las modalidades de phishing y otros ataques informáticos importantes para poder realizar el estudio monográfico.

Aunque existen diferentes definiciones asociadas a términos como *phishing*, *malware*, entre otros; los propuestos corresponden con las expectativas del presente trabajo de grado, de esta forma se define:

5.3.1 *Vishing*. Es el engaño que se realiza vía telefónica, donde el delincuente suplanta la identidad de algún funcionario de x empresa, solicitando datos confidenciales. El centro policial cibernético la define como la “Modalidad de estafa en la que los ciberdelincuentes aplican técnicas de ingeniería social vía telefónica, con el fin de tener acceso a información personal y financiera de sus víctimas para así lucrarse económicamente. Durante la vigencia se han recibido 1055 casos de *vishing* por cifras cercanas a los $2.132.000.000”. 53 A continuación, se ilustra el promedio de las víctimas, según los datos obtenidos.

53 POLICIA NACIONAL. Balance Cibercrimen en Colombia 2017. Colombia, 2017, Pág. 3 [en línea]. [Consultado: 19 de marzo de 2019] Disponible en: https://caivirtual.policia.gov.co/contenido/informe-balance-del-cibercrimen-2017

5.3.2 *Tabnabbing*. Desarrollado por el estadounidense Aza Raskinuno, conocido por su trabajo con Mozilla Firefox. 54 Este ataque actúa sobre las pestañas en reposo o que se dejan inactivas durante determinado tiempo, con el fin de suplantar una de esas páginas inactivas, informando que la sesión expiro y de tal forma la víctima acceda a diligenciar nuevamente los campos de usuario y contraseña.

5.3.3 *Smishing*. Es el engaño que se realiza por medio de mensajes de texto SMS, informando sobre algún premio que le hacen creer a la víctima que se ganó, solicitan por medio de él comunicarse con un número o ingresar a una página web, por medio de un enlace donde se le solicita información confidencial, un riesgo adicional es que puede descargarse un código malicioso en el celular, Según el balance Cibercrimen en Colombia 2017, del Centro Cibernético Policial, se reportaron 856 casos en 2017.

5.3.4 *Whaling*. También conocido como ataque BEC, se enfoca en suplantar a los altos directivos de las empresas, con el fin de dar órdenes falsas a los empleados, especialmente del área financiera, autorizando alguna transacción o pago de alguna cuenta pendiente. “El ‘whaling’ se está convirtiendo en un problema tal que, según el FBI, ya ha costado más de 2.300 millones de dólares (más de 2.000 millones de euros) a las empresas de casi 80 países diferentes que se han visto afectadas en los últimos tres años. Desde enero de 2015, el número de víctimas identificadas se han incrementado en un 270 %, entre ellas grandes y famosas compañías como Mattel, Snapchat o Seagate Technologies”55.

Adicionalmente, según el informe del centro cibernético policial[56], en el año 2019, los principales vectores de engaño para este ataque BEC fueron, 80% Spear *phishing*; 60% Suplantación de identidad; 53% *Spoofing*; 37% Infección de sitios frecuentemente visitados por los empleados. A través de la Figura 6 tomada del informe mencionado, se muestra cómo se realiza este ataque BEC, donde el gerente cae en el engaño del ciberdelincuente, permitiéndole obtener acceso a su email, luego desde el correo del gerente solicita a la funcionaria encargada del área

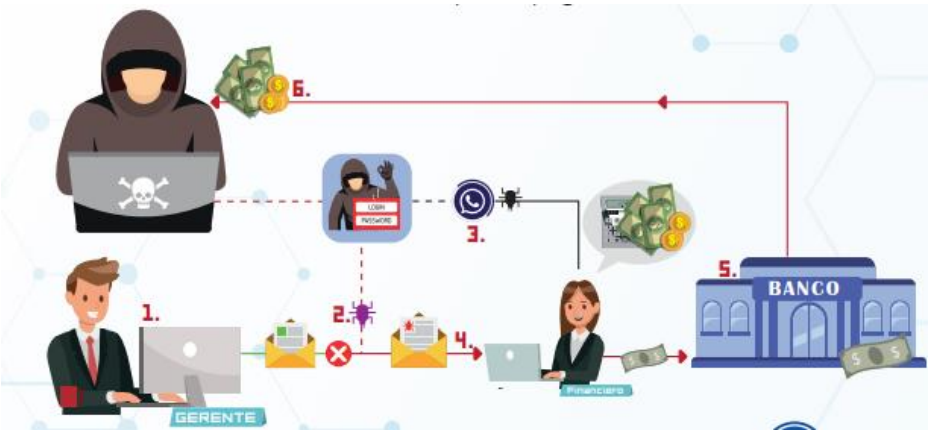
54 MOPOSITA GUANGASHI, Paul Fernando. “Medidas de protección informática para evitar el robo de identidad provocado por el ataque phishing “the Tabnabbing attack" para la facultad de ingeniería en sistemas, electrónica e industrial”. Ecuador, 2012, 176 páginas. Trabajo de grado (Ingeniero en Sistemas Computacionales e Informáticos.). Universidad técnica de Ambato. Facultad de ingeniería en sistemas, electrónica e industrial carrera de ingeniería en sistemas computacionales e informáticos. [En línea]. [Consultado: 19 de marzo de 2019]. Disponible en: http://repositorio.uta.edu.ec/handle/123456789/2378

55 PANDA. ‘Whaling’, el nuevo fraude que amenaza a tu empresa. 2016. [En línea]. (junio de 2016). [Consultado: 19 de marzo de 2019]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/whaling-amenaza-contra-empresas/

56 POLICIA NACIONAL y CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias Cibercrimen Colombia 2019-2020 [en línea]. Bogotá. Octubre 29 del 2019. 36 páginas. Primera edición [Consultado: 12 de julio de 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

financiera, realizar una transferencia; finalmente la realiza y llega a manos del cibercriminal.

Figura 6. Whaling



Fuente: POLICIA NACIONAL y CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias Cibercrimen Colombia 2019-2020 [en línea]. Bogotá. Octubre 29 del 2019. 36 páginas. Primera edición [Consultado: 12 de julio de 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

5.3.5 Spear Phishing. Este método se enfoca específicamente en atacar a una determinada empresa, los ciberdelincuentes realizan un análisis previo, de la empresa que será su próxima víctima y aprovechan cualquier vulnerabilidad, para realizar ingeniería social y seguidamente el ataque de *phishing*. Tiene similitud con el ataque BEC o *whaling*, ya que es un ataque dirigido. Sin embargo, el *Spear Phishing* se dirige a cualquier funcionario de la empresa y el whaling se dirige a los altos cargos de las entidades, es decir que, el *spear phishing* es un medio para ejecutar el *whaling*.

5.3.6 Malware. También conocido como software malicioso, pero dentro de ese término se incluyen todos los programas con código malicioso que daña, invade, cifra e inhabilita los sistemas informáticos, con diferentes fines.

Malware bytes siendo una empresa antimalware, son especialistas en estudiar estos programas maliciosos y dan una descripción de los más utilizados:

- El adware es un software no deseado diseñado para mostrar anuncios en su pantalla, con mayor frecuencia dentro de un navegador web. Por lo general, utiliza un método clandestino para disfrazarse de legítimo o se suma a otro programa para engañarlo para que lo instale en su PC, tableta o dispositivo móvil.

- El software espía es un malware que observa en secreto las actividades del usuario de la computadora sin permiso y lo informa al autor del software.

- Un virus es un malware que se adhiere a otro programa y, cuando se ejecuta (generalmente sin darse cuenta por parte del usuario), se replica modificando otros programas informáticos e infectándolos con sus propios fragmentos de código.

- Los gusanos son un tipo de malware similar a los virus, que se autorreplican para propagarse a otras computadoras a través de una red, y generalmente causan daños al destruir datos y archivos.

- Un troyano, o caballo de Troya, es uno de los tipos de malware más peligrosos. Por lo general, se presenta a sí mismo como algo útil para engañarte. Una vez que está en su sistema, los atacantes detrás del troyano obtienen acceso no autorizado a la computadora afectada. A partir de ahí, los troyanos se pueden utilizar para robar información financiera o instalar amenazas como virus y ransomware.

- El ransomware es una forma de malware que le bloquea el acceso a su dispositivo y / o cifra sus archivos, luego le obliga a pagar un rescate para recuperarlos. Ransomware se ha llamado el arma del delincuente cibernético de elección, ya que exige un pago rápido, rentable en difícil de traza criptomoneda. El código detrás del ransomware es fácil de obtener a través de mercados criminales en línea y defenderse contra él es muy difícil.

- Rootkit es una forma de malware que proporciona al atacante privilegios de administrador en el sistema infectado. Por lo general, también está diseñado para permanecer oculto al usuario, a otro software del sistema y al propio sistema operativo.

- Un keylogger es un malware que registra todas las pulsaciones de teclas del usuario en el teclado, generalmente almacena la información recopilada y la envía al atacante, que busca información confidencial como nombres de usuario, contraseñas o detalles de tarjetas de crédito.

- La minería de criptomonedas maliciosa, también denominada a veces minería no autorizada o criptojacking, es un malware cada vez más frecuente que suele instalar un troyano. Permite que otra persona use su computadora para extraer criptomonedas como Bitcoin o Monero. Entonces, en lugar de permitirle cobrar con la potencia de su propia computadora, los criptomineros envían las monedas recolectadas a su propia cuenta y no a la suya. Básicamente, un criptominero malicioso está robando sus recursos para ganar dinero.

- Los exploits son un tipo de malware que se aprovecha de errores y vulnerabilidades de un sistema para permitir que el creador del exploit tome el control. Entre otras amenazas, los exploits están vinculados a la publicidad maliciosa, que ataca a través de un sitio legítimo que, sin saberlo, extrae contenido malicioso de un sitio malicioso. Luego, el contenido malicioso intenta instalarse en su computadora en una descarga automática. No es necesario hacer clic. Todo lo que tienes que hacer es visitar un buen sitio en el día equivocado[57] .

5.3.7 Suplantación de identidad. Se da cuando un ciberdelincuente toma la identidad de una persona natural o jurídica para fines delictivos ya que puede cometer delitos en nombre de la persona suplantada, adicionalmente puede beneficiarse económicamente, robando los datos confidenciales y con estos realizar transacciones, tomar créditos o propiedades. También puede ejercer manipulación psicológica haciéndose pasar por un gran empresario o una figura de autoridad, con el fin de obtener datos importantes, transacciones que solicité, entre otros. Los profesores Luis Gabaldón y Wilmer Pereira en su artículo lo definen como "la suplantación del titular de un derecho o crédito por un impostor para obtener un beneficio injusto recibe cada vez más atención en materia de fraudes cometidos con la ayuda de las tecnologías de la información. Las consecuencias de la suplantación rebasan en muchos casos la pérdida económica directa del titular del derecho afectado, para comprometer su historia crediticia, su prestigio y hasta su identidad social"[58].

5.3.8 Spoofing. Consiste en suplantar páginas web y otras tecnologías de red que sean susceptibles de suplantación con el fin de capturar datos confidenciales, tal como se muestra en la Figura 7. Tiene diferentes tipos, algunos son: ataque IP *spoofing*, ARP *spoofing*, DNS *spoofing*, Web *spoofing*, e-mail *Spoofing*.

> Un ataque de *Spoofing* consiste en suplantar validadores, credenciales o identificadores estáticos, es decir, parámetros que permanecen invariables antes, durante y después de la concesión de un privilegio, una autentificación etc… los identificadores que se pueden suplantar mediante un ataque de *Spoofing* son los mostrados en la Figura 29. Para recopilar la información necesaria para hacer la suplantación de identificadores es necesaria una fase previa en la que se emplee algún tipo de ataque pasivo. Con este tipo de ataques, en concreto, el atacante puede, por ejemplo, mediante falsificación de información suplantar la identidad de algún usuario de la red WLAN[59].

---

[57] MALWAREBYTES. Software malicioso. [en línea]. [Consultado 13 de octubre de 2020]. Disponible en https://www.malwarebytes.com/malware/

[58] GABALDON, Luis Gerardo y PEREIRA Wilmer. Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico. En: DOSSIE. Porto Alegre. 2008. (27 p.) [Consultado: 14 de octubre de 2020]. Disponible en: https://www.scielo.br/pdf/soc/n20/a08n20.pdf

[59] ANDREU, Fernando; PELLEJERO, Izaskun y LESTA Amaia. Fundamentos y Aplicaciones de Seguridad en Redes WLAN: Fundamentos y Aplicaciones de Seguridad. [en línea]. Marcombo, 2006.

Figura 7. Spoofing.

Figura 29 Validadores suplantables mediante spoofing

ANDREU, Fernando; PELLEJERO, Izaskun y LESTA Amaia. Fundamentos y Aplicaciones de Seguridad en Redes WLAN: Fundamentos y Aplicaciones de Seguridad. [en línea]. Marcombo, 2006. 160p. ISBN 8426714056, 9788426714053. [Consultado: 14 de octubre de 2020]. Disponible en https://books.google.com.co/books?id=k3JuVG2D9lMC&dq=que+es+spoofing&hl=es&source=gbs_navlinks_s

5.3.9 DDOS. Un ataque DDOS se ejecuta mediante una red de computadores infectados con *malware,* conocidos generalmente como *botnet* o zombis, donde se ejerce un control total sin que el usuario lo sepa, para colapsar un servidor. El autor Peter D. Nyheim lo define como:

> Un ataque DDoS es cuando un cibercriminal u organización dirige una sobrecarga de tráfico de sitios web a su propiedad online, lo que causa que colapse. Típicamente llamado un ataque de denegación de servicios distribuido, este ataque bloquea la venta online al causar que su servidor colapse, interrumpiendo así su proceso de ventas. A causa de que sus consumidores no podrán acceder a su sitio y, por ende, a la compra de sus productos y servicios, simplemente se trasladan a sus competidores mientras usted se apura en tratar de resolver el problema[60].

160p. ISBN 8426714056, 9788426714053. [Consultado: 14 de octubre de 2020]. Disponible en https://books.google.com.co/books?id=k3JuVG2D9lMC&dq=que+es+spoofing&hl=es&source=gbs_navlinks_s

[60] PETER, Nyheim, Estrategias tecnológicas para la industria de la hostelería. [en línea]. Ediciones Universidad Católica de Salta, 2019. 276 p. ISBN 9506231818. [Consultado 14 de octubre de 2020]. Disponible en: https://books.google.com.co/books?id=TmK4DwAAQBAJ&dq=Ataque+DDOS&hl=es&source=gbs_navlinks_s

5.4 MARCO HISTÓRICO

> Antes de que se estableciera el término "phishing", se describió en detalle una técnica de phishing en un documento y una presentación entregados al Grupo Internacional de Usuarios de HP de 1987, Interex.
>
> El uso del nombre en sí se atribuye por primera vez a un notorio spammer y hacker a mediados de la década de 1990, Khan C Smith. Además, según los registros de Internet, la primera vez que el phishing se utilizó y registró públicamente fue el 2 de enero de 1996. La mención ocurrió en un grupo de noticias de Usenet llamado AOHell. En ese momento, America Online (AOL) era el proveedor número uno de acceso a Internet, con millones de inicios de sesión diarios[61].

A mediados de los años 90, se conocieron los primeros casos de *phishing,* los cuales fueron dirigidos a AOL, los ciberdelincuentes se hacían pasar por empleados de AOL y mediante correos electrónicos con asuntos como, por ejemplo, supuestas confirmaciones de facturas o verificaciones de cuentas lograban conseguir las contraseñas de los usuarios de AOL. Luego de obtener las contraseñas y por lo tanto tener el control de las cuentas, eran utilizadas para enviar spam u otras actividades cibercriminales. Ante este problema del *phishing*, AOL tomo diferentes medidas eficaces, una de ellas fue informar a sus clientes que ningún empleado podría solicitar información confidencial a los usuarios.

Sin embargo, este ataque de *phishing* fue esparciéndose a otras organizaciones especialmente financieras y servicios de pagos en línea. Inicialmente los correos de *phishing* podían ser identificados por los errores ortográficos, pero cada vez iban mejorando sus técnicas, a tal punto que registraron docenas de dominios que falsificaron eBay y PayPal pasándose por los sitios web reales, los clientes de PayPal recibieron correos de *phishing*, solicitando información confidencial, como los números de tarjetas o cuentas. El primer ataque de phishing conocido contra un banco lo informó The Banker (una publicación propiedad de The Financial Times Ltd.) en septiembre de 2003. Un informe de 2007 de Gartner que indica que hasta 3.6 millones de adultos perdieron $ 3.2 mil millones entre agosto de 2006 y agosto de 2007.

.

“En Colombia cada mes se registran cerca de 187 denuncias por robos informáticos, entre ellos el *phishing* es el delito más común. Su popularidad ha crecido velozmente en el país, evidencia de esto son los cerca de 6 millones de dólares que se perdieron en el 2011 a causa de este delito”[62]. Una de las páginas más atractivas para los cibercriminales es la página del *Facebook*, según SecureList fue una de las tres más atacadas el año pasado. Durante el primer trimestre del 2018 realizo un

[61] Ibíd., p. 8.
[62] ASOSEC. El Phishing en Colombia. 2013. [En línea]. [Consultado: 5 de mayo de 2019]. Disponible en: http://asosec.co/2013/03/el-phishing-en-colombia/

reporte de “las categorías financieras en su conjunto (bancos, 18,25%; tiendas en línea, 17,26%; sistemas de pago, 8,41%) todavía representan casi la mitad de todos los ataques, el 43,92%, que son 4,46 puntos porcentuales más que el último trimestre. Les siguen las categorías “Organizaciones gubernamentales” con el 4,75%; “Redes sociales y blogs” con el 4,11%, “Empresas de telecomunicaciones” con el 2,47%, “Empresas informáticas” con el 1,55%, “Programas de mensajería”, con el 0,66%; “Juegos en línea”, con el 0,43% y “Líneas aéreas” con el 0,07%” [63]. Esta información detallada se ilustra en la Figura 8.

Figura 8. Ataques de *Phishing* SecureList 2018

Phishing en Colombia

No. Denuncias Mensuales	Peridadas Millones Dolares
187	6.000.000

Analisis Durante Primer Trimestre año 2018 Fraudes Financieros

		Refrencia al Ultimo Trimestres	
Concepto	**Indicador %**	**Incremento**	**Tendencia**
Bancos	18,25%		
Tienda Linea	17,26%		
Sistemas de Pagos	8,41%		
Totales	**43,92%**	**4,46%**	⬆

Concepto	Indicador %
Organizaciones guberna	4,75%
Redes sociales y blogs	4,11%
Empresas de telecomuni	2,47%
Empresas informáticas	1,55%
Programas de mensajerí	0,66%
Juegos en línea	0,43%
Líneas aéreas	0,07%

Fuente: Autor, con base en, SECURELIST. El Spam y el *phishing* en 2018. [En línea]. [Consultado: 5 de mayo de 2019]. Disponible en https://securelist.lat/spam-and-*phishing*-in-q1-2018/86992/

Existen muchos casos de *phishing*, en diferentes sectores y diferentes modalidades, lo que demuestra que, cualquier persona puede ser víctima de *phishing*, incluso sin acceso a internet, ya que por ejemplo, en la modalidad de *vishing*, el ataque se realiza a través de una llamada telefónica y en la misma medida que avanza la tecnología, avanzan las técnicas de los ciberdelincuentes, creando nuevas modalidades de estafa y de explotación de vulnerabilidades tanto de los sistemas informáticos, como de los usuarios.

[63] SECURELIST. El Spam y el phishing en 2018. [En línea]. [Consultado: 5 de mayo de 2019]. Disponible en https://securelist.lat/spam-and-phishing-in-q1-2018/86992/

5.5 MARCO LEGAL

En Colombia se han implementado leyes enfocadas a la seguridad digital, de la información y de los usuarios, lo que permite un crecimiento del derecho informático en el país, permitiendo penalizar los delitos informáticos y bridando seguridad a los usuarios. Las siguientes son algunas de las más reconocidas.

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

- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Habeas 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.

- Decreto 1727 de 2009 Por el cual se determina la forma en la cual los operadores de los bancos de datos de información financiera, crediticia, comercial, de servicios y la proveniente de terceros países, deben presentar la información de los titulares de la información.

- Ley 1581 de 2012 Por la cual se dictan disposiciones generales para la Protección de Datos Personales.

- Ley 1621 de 2013 Por medio de la cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión constitucional y legal y se dictan otras disposiciones.

- 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.

- Código Penal Colombiano. Ley 599 de 2000.

- 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. En la siguiente normativa se realiza un énfasis especial, por ser de gran importancia y relevancia para esta monografía:

- Convenio de Budapest: Ley 1928 de julio 20 de 2018 "por medio de la cual se aprueba el convenio sobre la ciberdelincuencia, adoptado el 23 de noviembre de 2001, en Budapest. Acuerdo internacional, donde hacen parte diferentes países, buscando estandarizar los delitos informáticos con la finalidad de penalizarlos en

cualquiera de estos, convirtiéndose en una herramienta jurídica importante para los países que lo componen. Colombia se adhiere a este convenio en el año 2020 y de esta manera, da un gran paso, para la lucha contra la ciberdelincuencia, colaboración internacional y mejora de la seguridad digital del país. En el CONPES 3721 y 3854 se realizó la recomendación de que, Colombia se adhiriera a este acuerdo, debido al gran fortalecimiento y avance que representa para la ciberseguridad de Colombia.

- Ley 1273 del 2009 de la protección de la información y de los datos: Esta ley tipifica los delitos informáticos y los sanciona, se crea en una modificación del código penal colombiano. Ya que penaliza de los ciberdelitos y es muy importante para esta monografía, porque en ella habla claramente sobre las sanciones estipuladas para los cibercriminales. El *phishing* y sus modalidades puede ser un medio, un proceso o un paso que es utilizado para cometer los diferentes ciberdelitos tipificados en esta ley, es decir, haciendo uso del *phishing*, se puede descargar cualquier tipo de malware que, conlleva a la ejecución de los otros delitos informáticos, que esta ley contempla, los cuales son:

- Artículo 269A: Acceso abusivo a un sistema informático.

- Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación.

- Artículo 269C: Interceptación de datos informáticos.

- Artículo 269D: Daño Informático.

- Artículo 269E: Uso de software malicioso.

- Artículo 269F: Violación de datos personales.

- Artículo 269G: Suplantación de sitios web para capturar datos personales.

- Artículo 269H: Circunstancias de agravación punitiva.

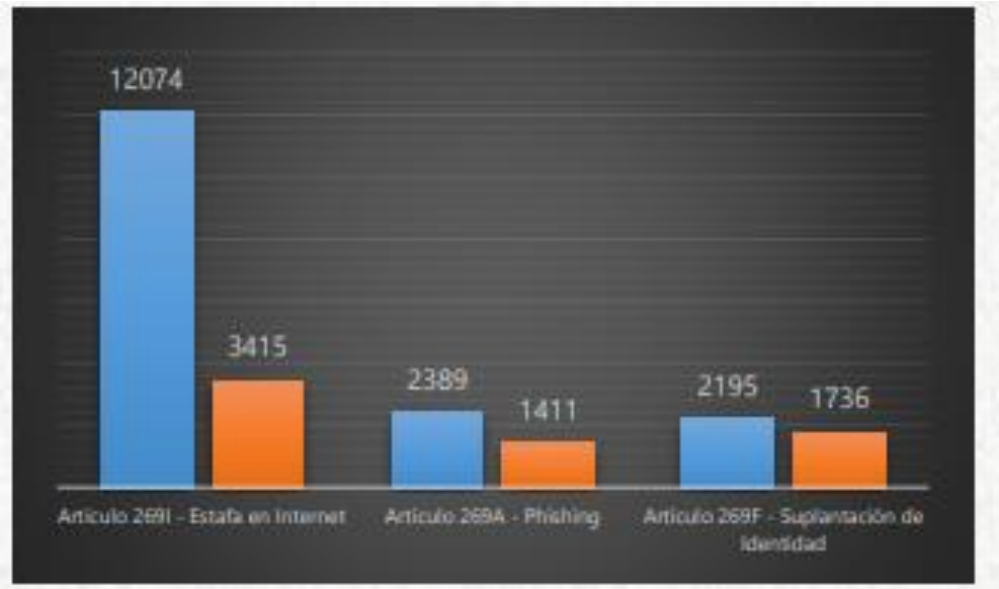
- Artículo 269I: Hurto por medios informáticos y semejantes.

- Artículo 269J: Transferencia no consentida de activos.

Como se muestra en la Figura 9 comparativa, realizada por el centro cibernético policial, de acuerdo con un informe del 2017; donde se comparan las cifras de 3 modalidades de incidentes informáticos, con cifras de 3 delitos que se encuentran enmarcadas dentro de las conductas punibles tipificadas en el Código Penal, cifras

reportadas en 2016. Adicionalmente, este mismo informe afirma que, el 76% de las infecciones de *Ransomware* se da a través del correo electrónico y spam.

Figura 9. Comparativo modalidad y delito



POLICIA NACIONAL. Amenazas del Cibercrimen en Colombia 2016-2017. [En línea]. Marzo de 2017. [Consultado 5 de mayo de 2019]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

Sin embargo, el artículo que, en consideración de la autora, mejor aplica en cuanto al delito de *phishing* es el artículo 269 G donde dice:

> Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave. En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave. La pena señalada en los dos incisos anteriores se agravará de

una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito[64].

- CONPES 3701 Lineamientos de Política para Ciberseguridad y Ciberdefensa: Este documento es de gran importancia, ya que, se crean diferentes grupos estatales, como por ejemplo el grupo de respuesta a incidentes – colCERT; Centro Cibernético Policial, con el fin de estar preparados en cuanto la ciberseguridad y ciberdefensa de Colombia.

- CONPES 3854 Política Nacional de Seguridad Digital: Dentro de todos los beneficios que busca implementar esta política, destacó la importancia que identifica sobre, la necesidad de implementar un modelo de gestión de riesgos, enfocado a los incidentes digitales.

- Norma ISO Sistema de Gestión de la Seguridad de la Información 27001 y 27002.

Colombia se ha destacado por sus avances legales frente a la seguridad de la información y ciberdefensa del país, sin embargo, aún existen vacíos jurídicos en la legislación colombiana, por lo tanto, en muchos existe impunidad para los ciberdelincuentes, debido al desconocimiento sobre los ciberdelitos por parte de los funcionarios que ejercen la función de penalizarlos. Sin embargo, es muy probable que la adhesión a este acuerdo ayude a mejorar la seguridad digital del país. Ya que cada vez es más necesario para el sistema penal del país familiarizarse con los ciberdelitos.

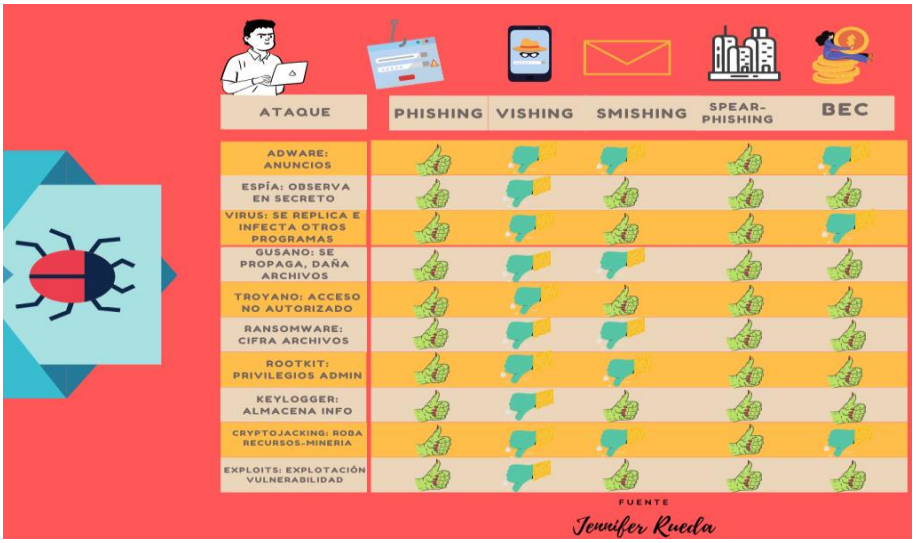
[64] COLOMBIA, SECRETARÍA JURÍDICA DISTRITAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C. LEY 1273 DE 2009. [En línea]. [Consultado: 15 de junio de 2019] Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

6. RESULTADOS

6.1 CLASIFICACIÓN DE LAS MODALIDADES DE *PHISHING* UTILIZADAS EN COLOMBIA FRENTE A LA CONCURRENCIA Y FINALIDAD DE USO DE LOS CIBERDELINCUENTES

6.1.1 Modalidad. Los ciberdelincuentes se valen de una gran variedad de ataques informáticos para lograr satisfacer sus deseos, en la actualidad existe un sin número de métodos, modalidades y programas maliciosos para llevarlo a cabo. Algunos requieren de más esfuerzo que otros y es por esto por lo que el *phishing* es tan apetecido por los delincuentes informáticos. El *phishing* y sus modalidades: a. *Smishing,* se describe como el engaño realizado por mensaje de texto; b*. Vishing,* engaño por medio de llamadas; c. S*pear-phishing,* ataques dirigidos y d. *BEC,* ataque dirigido a gerencia. Pueden utilizarse como un método único a la hora de robar datos confidenciales como primer paso, para finalmente robar dinero o si es deseo del ciberdelincuente puede utilizarlo como un medio para ejercer otro tipo de ataques informáticos, generalmente lo hacen cuando desean inyectar *malware* en el equipo informático. Dependiendo el *malware* que instalen será el daño que causen. En la Figura 10 se especifican las modalidades de *phishing* como único método y como medio para otros ataques informáticos, específicamente *malware*.

Figura 10. *Phishing* como medio – Malware

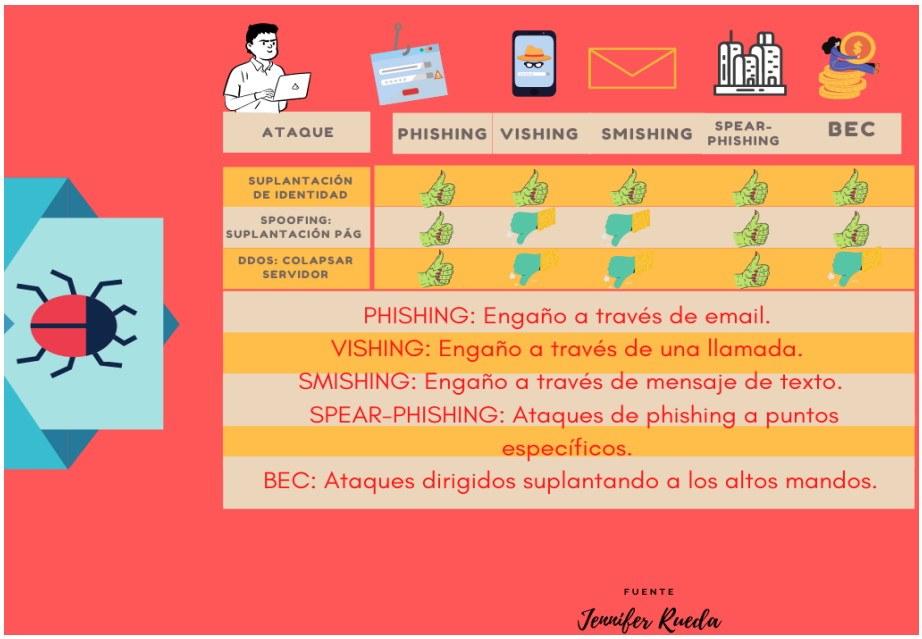


Fuente: Autor con base en, MALWAREBYTES. Software malicioso. [en línea]. [Consultado 13 de octubre de 2020]. Disponible en https://www.malwarebytes.com/malware/

Como se puede observar cuando el ciberdelincuente, desea instalar *malware*, utiliza las modalidades de *phishing* para conseguir su objetivo, una variante es la posible víctima, es decir, lo pueden dirigir a una persona aleatoriamente, pueden realizar un ataque de *phishing* dirigido a una organización específica o su víctima podría ser el nivel gerencial como lo es en el caso de los ataques BEC. Usualmente envían un email con un link o con un documento adjunto y al momento de ingresar al enlace o descargar el documento, se descarga el código malicioso. Aunque aparentemente la modalidad de *Vishing* no hace parte de esta línea para la instalación de *malware*, en ocasiones puede ser el primer paso, ya que, con esta modalidad es muy fácil obtener información confidencial y primordial para el ciberdelincuente, como la cuenta de correo electrónico donde se realizara el ataque de *phishing*. Es decir, un ataque conlleva a otro hasta lograr el objetivo final del delincuente informático.

En la Figura 11 se especifican las modalidades de phishing, utilizadas como medio para ejecutar otros ataques informáticos, como suplantación de identidad, *Spoofing* y ataque de denegación de servicios distribuido, también llamado DDOS por sus siglas en inglés *Distributed Denial of Service.*

Figura 11. *Phishing* como medio - otros ataques



Fuente: Autor con base en, MALWAREBYTES. Software malicioso. [en línea]. [Consultado 13 de octubre de 2020]. Disponible en https://www.malwarebytes.com/malware/

Se puede establecer con base en lo anterior que la modalidad de *Vishing*, el engaño por medio de una llamada telefónica es utilizada en la suplantación de identidad y aunque pareciera de menos importancia no lo es. Es muy común que las personas se dejen engañar por este medio, ya que, los delincuentes al ejercer el *vishing* en personas del común, suplantan la identidad de algún familiar que aparentemente necesita ayuda o se hacen pasar por una entidad bancaría, de telefonía. Entre otros. Cuando lo ejecutan hacia las organizaciones, suplantan la identidad de proveedores, clientes o entidades de autoridad y cuando el *vishing* es dirigido a la alta gerencia, suplantan la identidad del gerente o jefe de área de las organizaciones. Por lo tanto, aunque pareciera inofensivo, no lo es.
El *spoofing* generalmente es confundido con el *phishing* debido a que la modalidad es muy similar, más específicamente con el email-s*poofing y web-spoofing.* Sin embargo, el *spoofing* requiere de más habilidades técnicas. Por otro lado, los ataques DDOS se da por el colapso de los servidores frente a muchas solicitudes que llegan al tiempo desde una red de computadoras infectadas con *malware*.

6.1.2 Concurrencia y Finalidad. Teniendo claro que es el *phishing*, conociendo ya sus modalidades, se puede establecer inicialmente que una de las finalidades del *phishing* para los ciberdelincuentes, es que puede ser usado como medio para realizar otros ciberataques. Regularmente cuando un delincuente informático ataca a un usuario o una organización, su motivación tiene como fin un beneficio económico y claramente no les importa el daño psicológico y social que causan en el transcurso de la materialización del delito. Sin embargo, no es la única finalidad.

Cuando los ataques informáticos van dirigidos a las entidades del estado, la finalidad del ataque cambia, ya que, lo que busca el ciberdelincuente es reconocimiento, incrementar su ego y mostrar el control y poder que tiene para mostrar sus habilidades cibernéticas ilegales. Mostrando que puede violar los sistemas de seguridad informática y de la información, creyéndose superior. Adicionalmente, su intención es dañar la imagen del estado, ya que la sociedad entra a cuestionarse si el estado no tiene la capacidad de ciberdefensa y ciberseguridad que necesita un país.

Otra finalidad es, que el ciberdelincuente puede tener fines políticos, por ejemplo, los intentos que se han conocido sobre sabotajes en elecciones, el más conocido fue en las elecciones presidenciales de Estados Unidos en 2016 “se trataba de una oleada de correos dirigidos a miembros del Comité Nacional Demócrata y los miembros de la campaña de Clinton”[65]. Estos correos de *phishing* fueron enviados a varios miembros del partido demócrata de Hillary Clinton, capturando información confidencial de sus víctimas. En Colombia, el Centro de Comando y Control para la Ciberseguridad C4 informó a el periódico el tiempo que, “en el año 2018 en las elecciones del Congreso del 11 de marzo hubo 59.000 intentos de sabotaje

[65] BBC Mundo. 17 de diciembre de 2016. p.14 [consultado 15 de octubre de 2020]. Disponible en: https://www.bbc.com/mundo/noticias-internacional-38350244

digital”[66]. Además de los sabotajes, ante ataques informáticos a el estado buscan acceder a información confidencial, acceder abusivamente a los sistemas informáticos y en la actualidad muchos ataques se están centrando en la infraestructura crítica. Ante un ataque a un hospital, a el sistema de energía, donde pueda darse la pérdida de vidas humanas, se podría convertir en ciberterrorismo, porque genera miedo y afecta toda una población.

En la Tabla 2, se muestra con base en la información publicada en el CAI virtual del centro policial cibernético, los ataques informáticos utilizado por los ciberdelincuentes, con mayor concurrencia en los últimos cinco años en Colombia.

Tabla 2. Ataques más concurrentes

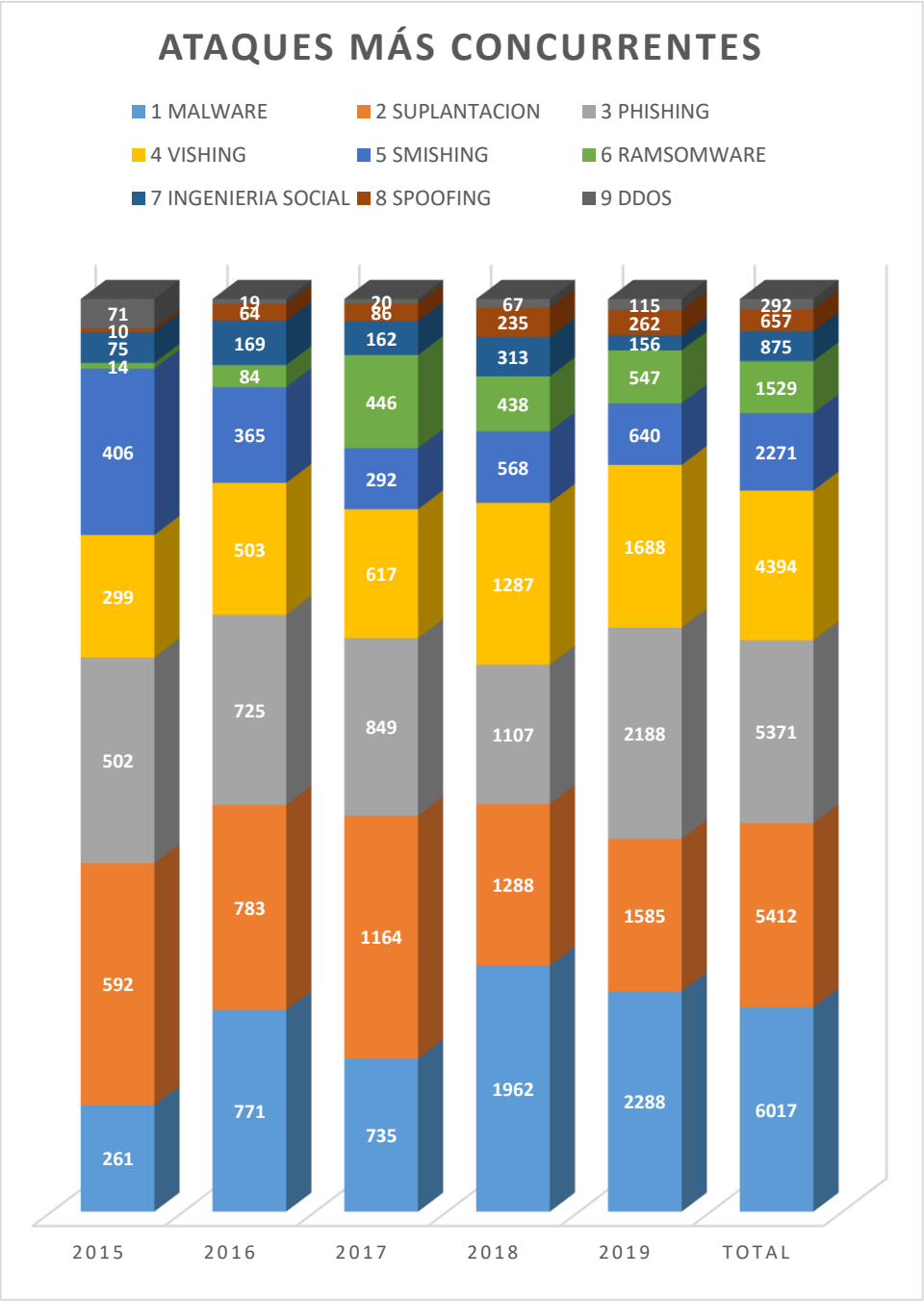
PUESTO	CIBERDELITO	2015	2016	2017	2018	2019	TOTAL
1	MALWARE	261	771	735	1962	2288	6017
2	SUPLANTACION	592	783	1164	1288	1585	5412
3	PHISHING	502	725	849	1107	2188	5371
4	VISHING	299	503	617	1287	1688	4394
5	SMISHING	406	365	292	568	640	2271
6	RAMSOMWARE	14	84	446	438	547	1529
7	INGENIERIA SOCIAL	75	169	162	313	156	875
8	SPOOFING	10	64	86	235	262	657
9	DDOS	71	19	20	67	115	292

Fuente: Autor con base en con base en, CENTRO CIBERNÉTICO POLICIAL. Ciberincidentes. [en línea]. [Consultado: 20 de junio de 2020]. Disponible en https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real

En la Figura 12, se realiza un análisis gráfico de los datos suministrados en la Tabla 2, facilitando la interpretación de las cifras obtenidas sobre los ataques informáticos más concurrentes, durante los últimos cinco años en Colombia.

Figura 12. Análisis de concurrencia

[66] El Tiempo. 26 de mayo de 2018. p. 7. [consultado 15 de octubre de 2020]. Disponible en: https://www.eltiempo.com/justicia/investigacion/ataques-a-pagina-web-de-la-registraduria-nacional-222756



Fuente: Autor con base en, CENTRO CIBERNÉTICO POLICIAL. Ciberincidentes. [en línea]. [Consultado: 20 de junio de 2020]. Disponible en https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real

De acuerdo con esta información se puede establecer que en los últimos cinco años los tres ataques más utilizados por los ciberdelincuentes en Colombia, es el *malware*

con 6.017 casos reportados, lo que quiere decir que en promedio cada año se reportaron 1.203 casos de *malware*. Así mismo la suplantación de identidad, ocupando el segundo lugar, reporto 5.412 casos para un promedio anual de 1.082 casos reportados. Como tercer lugar se encuentra el *phishing* con 5.371 casos reportados en los últimos cinco años, para un promedio de 1.074 reportes al año.

Adicionalmente en cuarto y quinto lugar, se encuentran las modalidades de *vishing* y *smishing* respectivamente, con un reporte de 4.394 casos de *vishing*, promedio anual de 878 casos y 2.271 reportes de smishing para un promedio de 454 casos reportados al año. El *ransomware* se encuentra en el sexto lugar con un reporte total en los últimos cinco años de 1.529 casos y con un promedio de 305 reportes cada año.

Por último, en el séptimo lugar está la ingeniería social con 875 reportes, promedio anual de 175 casos; el *Spoofing* obtuvo el puesto número ocho de la lista con 657 casos y promedio de 131 reportes por año; el ataque DDOS en el último puesto con 292 reportes con un promedio anual de 58 casos.

Se determina entonces que los ataques informáticos con mayor concurrencia en Colombia por los ciberdelincuentes, durante los últimos cinco años con base en la información del Centro Policial Cibernético son: el *malware*, la suplantación de identidad y el *phishing* y que la finalidad de uso de este ataque informático es la facilidad para ejecutar otros ataques, beneficios económicos, daño de reputación, sabotaje, acceso de información confidencial y mostrar poder y control.

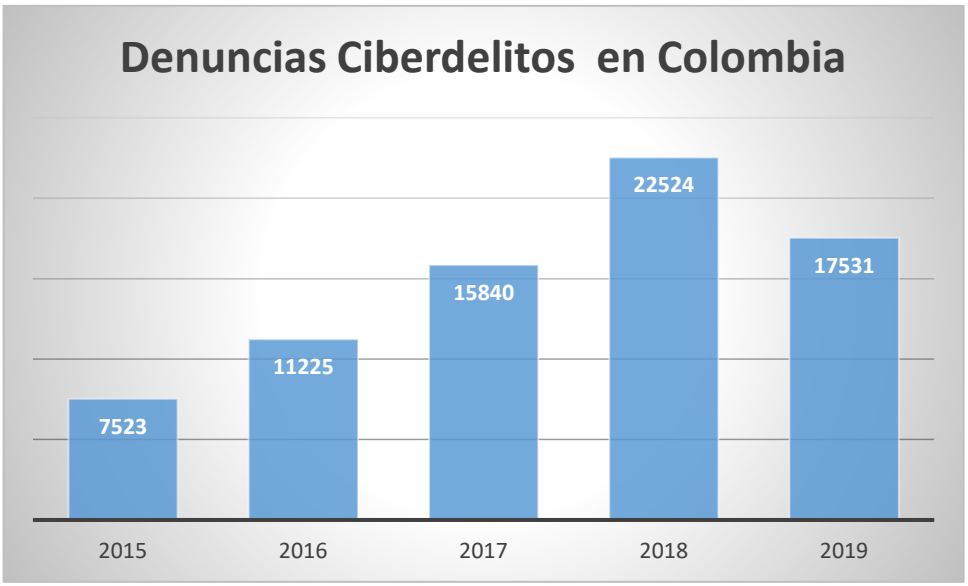
6.2 IMPACTO SOCIAL Y ECONÓMICO DEL PHISHING EN LOS SECTORES CON MÁS DENUNCIAS EN COLOMBIA DURANTE LOS ÚLTIMOS CINCO AÑOS.

6.2.1 Impacto Social. La confianza en el uso de los medios digitales es un factor muy importante en la actualidad para el desarrollo económico de un país. Colombia ha venido desarrollando diferentes estrategias, políticas y normatividad para la ciberseguridad y ciberdefensa del país, adicionalmente, el país se ha enfocado en fortalecer las instituciones del gobierno, apoyar al sector privado y al usuario del común. Sin embargo, el avance de los ataques informáticos llega más allá de los esfuerzos realizados y han impactado de forma negativa esta confianza digital en los usuarios y organizaciones del país. “La desconfianza en el uso del entorno digital puede estar relacionada con el uso no responsable del mismo, actitud que genera riesgos de seguridad digital que deben ser abordados eficientemente. Estos riesgos se reflejan en el incremento de las denuncias por delitos cibernéticos”[67].

[67] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3854. Op. cit., p.37.

El centro policial cibernético, reportó en el informe de tendencias cibercrimen en Colombia 2019-2020 las cifras de las denuncias desde el año 2015 hasta 2019, de los delitos informáticos, como se muestra en la Figura 13:

Figura 13. Denuncias ciberdelitos en Colombia

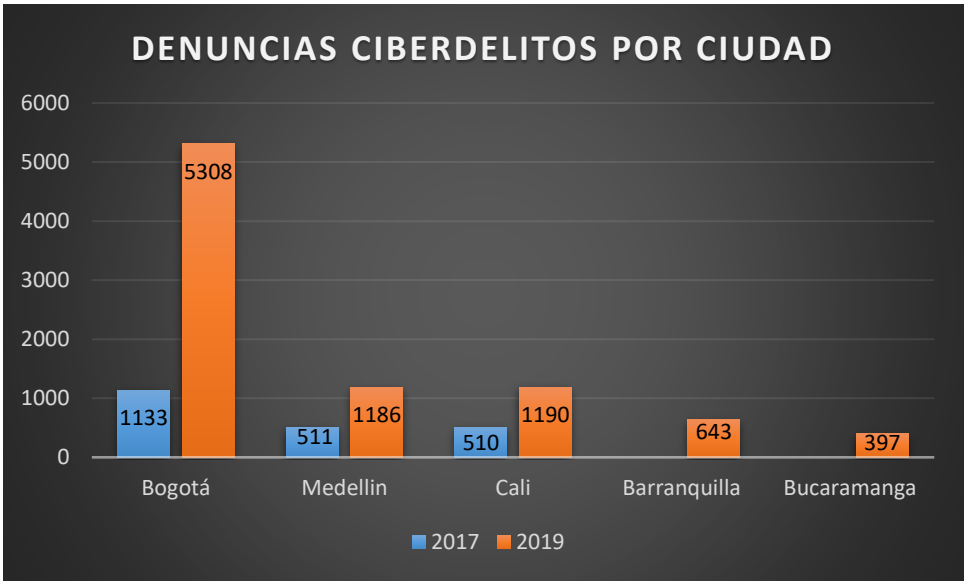


Fuente: Autor con base en, POLICIA NACIONAL y CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias Cibercrimen Colombia 2019-2020 [en línea]. Bogotá. Octubre 29 del 2019. 36 páginas. Primera edición [Consultado: 12 de julio de 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Se puede observar que el año con más ciberdelitos reportados en Colombia, fue en 2018 y que, desde 2015 hasta 2019, se viene incrementando las denuncias; aunque de 2018 a 2019 hubo un decremento del 22,16%, a nivel general, han ido aumentando las cifras. Es decir, que en los últimos cinco años 74.645 usuarios en Colombia, fueron víctimas de ataques informáticos, en promedio 14.929 víctimas por cada año.

En la Figura 14, se muestran las cifras de denuncias por delitos informáticos, clasificados por las ciudades más afectadas, en el año 2017 y 2019. Según la información obtenida del Centro Policial Cibernético.

Figura 14. Denuncias de ciberdelitos por ciudad



Fuente: Autor con base en, POLICIA NACIONAL y CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias Cibercrimen Colombia 2019-2020 [en línea]. Bogotá. Octubre 29 del 2019. 36 páginas. Primera edición [Consultado: 12 de julio de 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Mediante la figura anterior, se puede observar el incremento de las denuncias, por las ciudades más afectadas, especialmente en Bogotá con 5.308 casos, seguido por Medellín y Cali. Complementariamente con los datos obtenidos de la Fiscalía General de la Nación[68], con corte hasta septiembre del 2018, en los archivos de noticias criminales en el Sistema Penal Oral Acusatorio (SPOA), se encuentra el conteo de víctimas. Al clasificar los delitos, para determinar la ciudad más afectada por suplantación de sitios web para capturar datos personales, se determinó que, durante este periodo de tiempo, Bogotá, Medellín y Jamundí en el Valle del Cauca, fueron las más afectadas, como se muestra en la Figura 15.

[68] FISCALIA GENERAL DE LA NACIÓN. Datos abiertos de la Fiscalía General de la Nación. [en línea]. [Consultado: 15 agosto 2020]. Disponible en https://www.fiscalia.gov.co/colombia/gestion/estadisticas/

Figura 15. Ciudades más afectadas por *phishing* en Colombia -SPOA

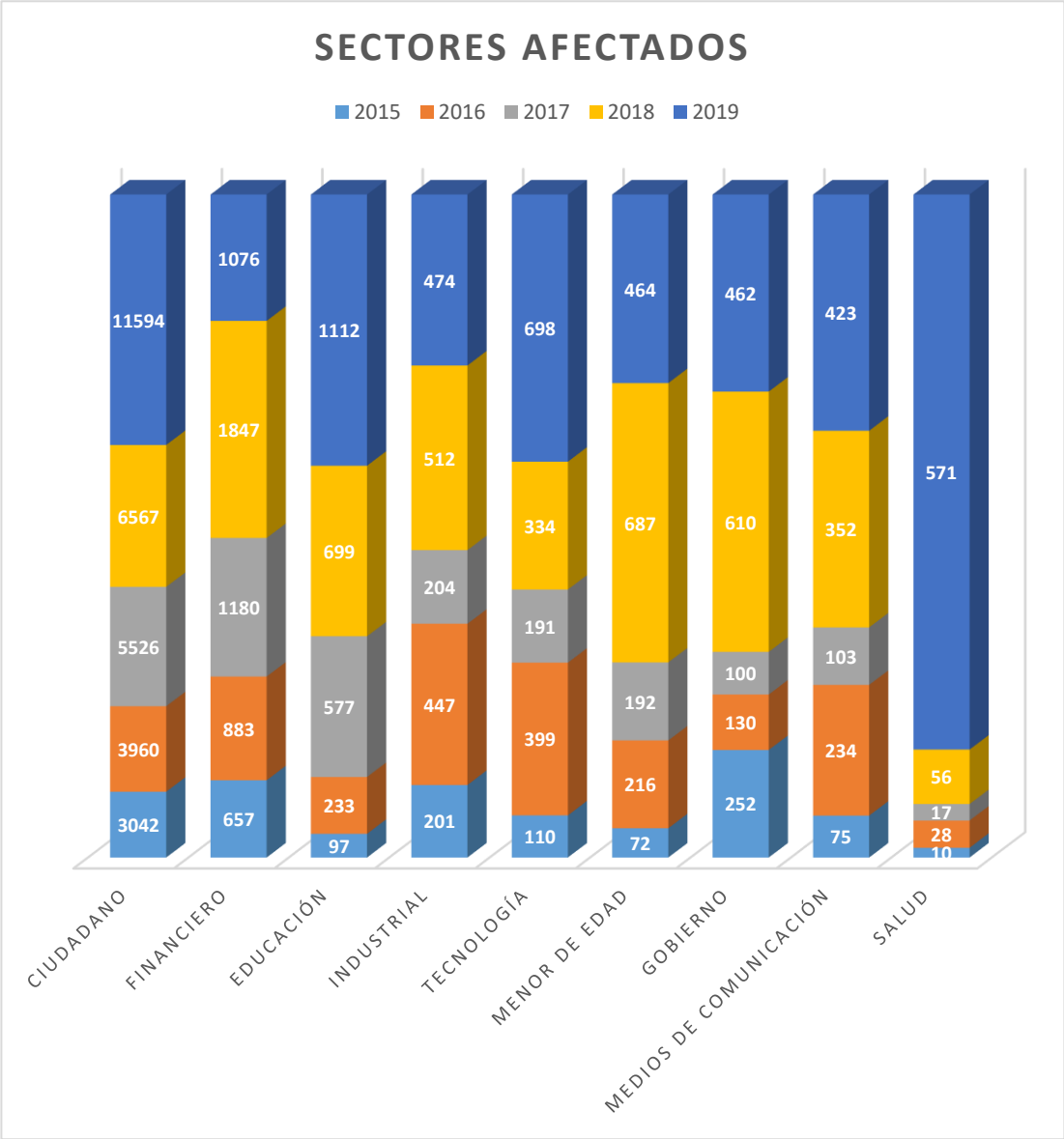
Victimas Clasificando los Delitos

AÑO	NÚMERO ANUAL DE CASOS	CIUDAD MÁS AFECTADA	Nro. Denuncias en Cuidad Más Afectada
2013	37	Medellín	9
2014	49	Medellín	14
2015	48	Medellín	11
2016	53	Jamundí	6
2017	132	Bogotá	18

Fuente: Autor con base en, FISCALIA GENERAL DE LA NACIÓN. Datos abiertos de la Fiscalía General de la Nación. [en línea]. [Consultado: 15 agosto 2020]. Disponible en https://www.fiscalia.gov.co/colombia/gestion/estadisticas/

Las cifras reportadas por el Centro Policial Cibernético y por la Fiscalía General de la Nación coinciden en que las ciudades con más denuncias por ataques informáticos son Bogotá, Medellín y Cali. Al clasificar por años desde 2015 hasta el 2019 y por sectores, estas denuncias generales de ciberataques en Colombia, con base en las cifras del mapa de calor publicado en la página del CAI virtual del Centro Policial Cibernético, se obtiene el siguiente resultado en la Figura 16.

Figura 16. Sectores más afectados por ataques informáticos en Colombia.



Fuente: Autor con base en, CENTRO CIBERNÉTICO POLICIAL. Ciberincidentes. [en línea]. [Consultado: 20 de junio de 2020]. Disponible en https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real

Como se puede evidenciar, el sector más afectado es el ciudadano con un reporte total en los últimos cinco años de 30.689, con un promedio de 6.137 denuncias cada año; en segundo lugar, se encuentra el sector financiero con total de 5.643 del año

2015 al 2019 y un promedio anual de 1.128 denuncias y como tercer lugar está el sector de la educación, con un total de reportes de 2.718 para un promedio de 543 reportes.

Asimismo, el sector industrial se encuentra en el cuarto lugar, con un total de denuncias de 1.838 y un promedio por año de 367; seguido por el sector de tecnología en el puesto quinto, con 1.732 denuncias, promedio anual de 346. En sexto lugar los menores de edad presentan 1.631 reportes en los últimos cinco años, lo que quiere decir que en promedio cada año 326 menores de edad fueron víctimas de un ataque informático.

Los tres sectores con menos denuncias fueron el sector gobierno con un total de 1.554, promedio anual de 310 reportes; los medios de comunicación con un total de 1.187 denuncias para un promedio de 237 reportes cada año y finalmente el sector salud con un total de denuncias desde el año 2015 hasta el año 2019 con 682 casos, promedio de 136 denuncias cada año.

De acuerdo con el Reporte Ciberseguridad 2020 del BID y la OEA “el cibercrimen y los ciberataques socavan la confianza de los usuarios en la economía digital. Las encuestas indican que, de la población mundial con acceso a Internet, menos del 50% confía en que la tecnología mejorará sus vidas, lo que demuestra una creciente y profunda falta de confianza con respecto a la privacidad de los datos”[69]. Los ciberdelitos además de impactar negativamente en la confianza digital, afecta la reputación de los usuarios.

En un caso en que un ciberdelincuente suplante la identidad de una persona y la comprometa en un delito, daña el buen nombre de la persona suplantada y tendría que entrar a demostrar que su identidad fue suplantada. En el caso de los ataques dirigidos a organizaciones daña la credibilidad de sus clientes, además en caso de que se pueda establecer por donde ingreso el ataque informático, el personal responsable puede ser despedido y en caso de un ciberataque al estado, afecta su imagen ante toda la población.

Ahora bien, se ha establecido que los ataques informáticos impactan socialmente, la confianza digital y la reputación, pero también existe un impacto psicológico, “la magnitud del impacto psíquico asociado a una situación de victimización criminal estará modulada por distintos factores, que tradicionalmente se han agrupado en tres grupos: factores relacionados con el delito, factores de protección o resiliencia y factores de vulnerabilidad (Echeburúa et al., 2004). A partir de los criterios de la

[69] Banco Interamericano de Desarrollo y Organización de los Estados Americanos. Ciberseguridad Riesgos, Avances Y El Camino A Seguir En América Latina Y El Caribe [en línea]. BID. 2020. [Consultado: 16 de octubre de 2020]. Disponible en: https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/BID%20-%20OEA%20Reporte-Ciberseguridad-2020-riesgos-.pdf?ver=1601971104202

teoría del estrés, se han descrito tres fases en la evolución del daño psíquico derivado de una situación de victimización criminal"[70]. Lo anterior se describe en la Figura 17.

Figura 17. Evolución del daño Psíquico

Tabla 1
Fases en la evolución del daño psíquico (elaboración propia a partir de Soria, 2005)

Fase	Duración	Características
Shock o desorganización	De minutos a horas (reacción inmediata)	Shock activo: agitación, gritos, enturbiamiento de la conciencia, hiperactivación, deambulación.
		Shock pasivo: catatonía, paralización o hipoactividad motriz, deambulación, enturbiamiento de la conciencia.
Reorganización	De semanas a meses (reacción a corto plazo)	Tipo I: sintomatología traumática aguda.
		Tipo II: negación (reacción postraumática retardada).
Readaptación	Variable (6 meses a 2 años) (reacción a largo plazo)	Recuperación o cronificación de la sintomatología traumática.

Fuente: MUÑOZ, José Manuel. La evaluación psicológica forense del daño psíquico: propuesta de un protocolo de actuación pericial. En: Redalyc. [en línea]. Red de Revistas Científicas de América Latina, el Caribe, España y Portugal. Madrid, España. vol. 23, 2013, pp. 61-69. [Consultado: 16 de octubre de 2020]. Disponible en https://www.redalyc.org/pdf/3150/315028685010.pdf ISSN 1133-0740.

[70] MUÑOZ, José Manuel. La evaluación psicológica forense del daño psíquico: propuesta de un protocolo de actuación pericial. En: Redalyc. [en línea]. Red de Revistas Científicas de América Latina, el Caribe, España y Portugal. Madrid, España. vol. 23, 2013, pp. 61-69. [Consultado: 16 de octubre de 2020]. Disponible en https://www.redalyc.org/pdf/3150/315028685010.pdf ISSN 1133-0740.

Esto confirma que, ante un ataque de phishing, el usuario sufre un impacto negativo psicológico, especialmente en esta modalidad que hace parte de la ingeniería social, ya que, las personas entregaron su confianza al delincuente informático y obtienen pérdidas económicas, afectación en su reputación y buen nombre, inseguridad, desconfianza y posiblemente en los ataques dirigidos pueden perder el empleo. Además del traumatismo de realizar las denuncias correspondientes y todo el proceso que lleva tratar de que se haga justicia.

Se puede establecer entonces, que los ataques de *phishing* han impactado de una manera negativa a la sociedad, afectando a las víctimas en el aspecto psicológico, la confianza digital, el buen nombre de los usuarios, organizaciones y del estado. En Colombia durante los últimos cinco años 74.645 usuarios fueron víctimas de ataques informáticos, en consecuencia, sufrieron dicho impacto social, siendo Bogotá, Medellín y Cali las ciudades más afectadas y a su vez al ser clasificados por sectores, lo más afectados fueron los ciudadanos, el sector financiero y sector de educación.

6.2.2 Impacto Económico. Una de las finalidades principales del ataque de *phishing es* obtener un beneficio económico.

Como se puede evidenciar en las figuras anteriores, el impacto de los delitos informáticos en los sectores de nuestro país, han ido aumentado a través del tiempo, a medida que las técnicas de los ciberdelincuentes avanzan, junto con la tecnología. En la Tabla 3, se clasifican los sectores con el número total de denuncias reportadas, desde 2015 hasta 2019, con el fin de visualizar de manera ascendente, los sectores con mayor impacto.

Tabla 3. Sectores con mayor impacto

SECTOR	DENUNCIAS
CIUDADANO	30689
FINANCIERO	5643
EDUCACIÓN	2718
INDUSTRIAL	1838
TECNOLOGÍA	1732
MENOR DE EDAD	1631
GOBIERNO	1554
MED. COMUNICACIÓN	1187
SALUD	682

Fuente: Autor con base en, CENTRO CIBERNÉTICO POLICIAL. Ciberincidentes. [en línea]. [Consultado: 20 de junio de 2020]. Disponible en https://caivirtual.policia.gov.co/ciberincidentes/tiempo-real

Entre los años 2015 y 2019, con base en la Figura 18 se muestra que el porcentaje de phishing fue alrededor del 42%, cuyo rango de costo por empresa denunciado oscilaba entre $300.000.000 y $ 5.000.000.000 para una estimación promedio de $2.350.000.000. Lo cual muestra el promedio de pérdidas económicas en las organizaciones colombianas, de acuerdo con en el rango de las cifras denunciadas se puede establecer que los ataques de phishing afectan cualquier tipo de empresa, abarcando desde las MiPymes, Pymes hasta las de grandes capitales.

Figura 18. Impacto económico del phishing.

AÑO	2015	2016	2017	2018	2019
TOTAL DENUNCIAS	7.523	11.225	15.840	22.524	15.948
PISHING	42%	42%	42%	42%	42%
DENUCNIAS PISHING	3160	4715	6653	9460	6698
COSTOS POR EMPRESA MÍNIMO DENUNCIADO	$ 300.000.000	$ 300.000.000	$ 300.000.000	$ 300.000.000	$ 300.000.000
COSTOS POR EMPRESA MÁXIMO DENUNCIADO	$ 5.000.000.000	$ 5.000.000.000	$ 5.000.000.000	$ 5.000.000.000	$ 5.000.000.000
Estimación promedio	$ 2.350.000.000	$ 2.350.000.000	$ 2.350.000.000	$ 2.350.000.000	$ 2.350.000.000
ESTIMACION TOTAL	$ 7.425.201.000.000	$ 11.079.075.000.000	$ 15.634.080.000.000	$ 22.231.188.000.000	$ 15.740.676.000.000
Valores en Billones	$ 7,43	$ 11,08	$ 15,63	$ 22,23	$ 15,74
%PIB	0,0009%	0,0013%	0,0017%	0,0023%	0,0015%
PIB en precios Corrientes (Billones)	$ 804.692	$ 863.782	$ 920.471	$ 985.931	$ 1.062.342

Fuente: Autor con base en, POLICIA NACIONAL y CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias Cibercrimen Colombia 2019-2020 [en línea]. Bogotá. Octubre 29 del 2019. 36 páginas. Primera edición [Consultado: 12 de julio de 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Asimismo, las denuncias generales de ataques informáticos aumentaron en un 49,20% correspondiente a 3.702 denuncias entre 2015 a 2016, mientras que del 2016 a 2017 aumentaron con 4.615 denuncias correspondientes al 41,11% y de 2017 a 2018 incrementaron con 6.684 denuncias, correspondiente al 42,19%, a diferencia de 2018 a 2019 se redujeron las denuncias con 6.576 correspondiente al 29,19%. Las variaciones de los ataques informáticos mostraron un ascenso entre el año 2015 y 2018, pero en el año 2019 ocurrió un evento contrario ya que se dio un decremento importante, en consecuencia, con la respuesta oportuna a 12.879 incidentes por parte del Centro Policial Cibernético ya que no fue necesario llegar a instancias en la Fiscalía. Esto demuestra que la identificación y tratamiento de los

incidentes de seguridad en el momento preciso ayuda a controlar el impacto de los ataques informáticos.

Adicionalmente, las denuncias de phishing entre 2015 a 2016 incrementaron con una cifra de 1.555 denuncias correspondiente a un valor porcentual del 49,20%, de 2016 a 2017 el aumento en denuncias fue de 1.938 con porcentaje respectivo de 41,10% y entre 2017 a 2018 incrementaron con 2.807 denuncias para un valor porcentual de 42,19%, finalmente en el periodo 2018 a 2019 la reducción fue de 2.760 denuncias, correspondientes al 29,19%. Dentro de la tipificación de los ataques informáticos, el *phishing* ha generado un impacto negativo del 42%, mostrando la magnitud del daño que causó en los últimos cinco años, del orden de 22 billones de pesos, teniendo en cuenta el progresivo aumento de conectividad en las organizaciones colombianas y los avances tecnológicos, debe preverse las grandes pérdidas que puede seguir causando este ataque sino se toman las medidas necesarias para su mitigación. “Los datos disponibles respaldan estas preocupaciones; se estima que los daños por delitos cibernéticos alcanzarán los US$6 billones para 2021, lo que equivale al producto interno bruto (PIB) de la tercera economía más grande del mundo”[71].

6.3 VULNERABILIDADES MÁS COMUNES DE SEGURIDAD INFORMÁTICA EN LOS SECTORES CON MAYORES DENUNCIAS EN COLOMBIA

Teniendo en cuenta que la ciudadanía, el sector financiero y el sector educación son los sectores que encabezan la lista de los nueve sectores más afectados en Colombia por los ataques informáticos, se establecen las vulnerabilidades más comunes de seguridad informática en dos grupos, el ciudadano y las organizaciones.

Para empezar, es preciso conocer el significado de vulnerabilidad, una vulnerabilidad es un defecto en un sistema informático que al dejarlo desprotegido pone en riesgo la seguridad de la información pudiendo permitir que un ciberdelincuente infrinja los pilares de la integridad, disponibilidad y confidencialidad de esta.

El ciudadano en la mayoría de los casos conoce poco sobre las vulnerabilidades de seguridad informática a las que se encuentra expuesto y, por tanto, no conoce que podría hacer para mejorar esta situación, esto quiere decir como primera instancia que la principal vulnerabilidad del ciudadano es el desconocimiento.

Adicionalmente las personas que tienen un nivel de conocimiento sobre las vulnerabilidades informáticas no invierten dinero en adquirir programas originales

[71] Banco Interamericano de Desarrollo y Organización de los Estados Americanos**, Op. cit., p. 6.**

que le permitan obtener seguridad para su equipo e información, como son los antivirus, antimalware y por el contrario descargan programas de páginas desconocidas donde fácilmente se podría adquirir un *malware*, cediendo el control de su equipo y entregando su información confidencial, además muchas personas tienen por costumbre comprar programas piratas, creyendo que están beneficiando su economía, no prevén las consecuencias y se sienten seguros con versiones gratuitas de treinta días ofrecidas en las páginas de antivirus, no se tiene una conciencia de la magnitud del impacto que puede generarle un ataque informático. Por lo tanto, como segunda vulnerabilidad se establece la falta de inversión.

Asimismo, la ciudadanía no tiene el hábito de buenas prácticas enfocadas a la seguridad de la información, es decir realizar la actualización permanente del sistema operativo, realizar cambio de claves periódicamente, utilizar contraseñas seguras e intransferibles, no abrir correos sospechosos, no entregar información confidencial a personas desconocidas, especialmente nuestra cultura colombiana que es dada a ser muy social, en consecuencia la tercera vulnerabilidad es la ausencia de buenas prácticas respecto a la seguridad informática.

Ahora bien, frente a las vulnerabilidades más comunes de seguridad informática en las organizaciones, al igual que en los ciudadanos de a pie, la primera vulnerabilidad radica en que el nivel gerencial no invierte lo suficiente en herramientas y personal especializado en seguridad informática. Para tomar cualquier acción frente a los ataques informáticos, es necesario que se invierta en el área de seguridad informática, se necesita contar con equipos de tecnología, programas informáticos y personal capacitado para tener la capacidad de gestionar un incidente de seguridad que se pueda presentar en la organización. “Al analizar los valores de las empresas colombianas que asignaron algún presupuesto a la seguridad digital, se observó que la mediana del presupuesto de la seguridad digital en relación a las ventas de las empresas fue aproximadamente 0,3% del as ventas en 2016. Es decir, cuando se asignó presupuesto a la seguridad digital, este presupuesto no llegó al 1% de las ventas de la empresa en 2016”[72]. La falta de inversión en la seguridad digital no permite identificar los incidentes de seguridad, este factor es desconocido ya que no tienen la capacidad para reconocerlo.

Por otro lado, la segunda vulnerabilidad es la ausencia de un sistema de gestión de seguridad de la información que conlleva a la creación de una política de seguridad de la información efectiva, implementación de controles y buenas prácticas, las cuales permiten identificar los activos de la organización, las amenazas, vulnerabilidades y riesgos a los que se encuentra expuestos.

Contar con personal exclusivo para el área de seguridad informática es indispensable, ya que son las personas que están capacitadas para identificar las

[72] Banco Interamericano de Desarrollo; Ministerio de Tecnologías de la Información y las Comunicaciones y Organización de los Estados Americanos. Op. cit., p.60

vulnerabilidades y darles manejo, realizando una configuración segura del firewall, manteniendo los parches de seguridad actualizados, dando una buena funcionalidad al antivirus y a las demás herramientas de seguridad informática que tenga la organización. Por lo tanto, la falta de personal exclusivo para el área de seguridad informática es la tercera vulnerabilidad más común en las organizaciones. "El 44% de los entrevistados tenía solo entre 1-2 empleados, el 27% entre 3-5 personas y el 29% indicaron que tenían más de 5. Estos resultados enfatizan la necesidad de examinar cómo se está abordando el tema de la seguridad digital dentro de las entidades estatales. Algunos han argumentado que cuando se juntan las dos áreas, los puntos de vista de un departamento de TI varían desde el punto de vista de la seguridad en relación con las medidas proactivas y reactivas que una entidad debe implementar"[73].

6.4 ESTRATEGIAS Y CONTROLES PARA LA MITIGACIÓN DEL *PHISHING* RECOMENDADAS EN LAS POLÍTICAS PÚBLICAS RELACIONADAS CON LA SEGURIDAD INFORMÁTICA EN COLOMBIA.

Los ataques de *phishing* han afectado todos los sectores de la sociedad, desde los menores de edad, hasta el gobierno, por lo tanto, "Con el fin de abordar las incertidumbres, los riesgos, las amenazas, las vulnerabilidades y los incidentes digitales, en el 2011, el Gobierno nacional expidió el Documento CONPES 3701 Lineamientos de política para ciberseguridad y ciberdefensa. Esta política concentró los esfuerzos del país en contrarrestar el incremento de las amenazas informáticas que lo afectaban significativamente, y en desarrollar un marco normativo e institucional para afrontar retos en aspectos de seguridad cibernética"[74]. Se crea entonces, el colCERT con el fin de brindar apoyo al sector público y privado ante la respuesta a incidentes y con capacitaciones sobre seguridad de la información a cualquier sector; asimismo se creó el Comando Conjunto Cibernético - CCOC que está enfocado a la seguridad nacional, sin embrago uno de los objetivos es vincular al sector de educación ya que para ese momento existían pocas universidades donde dieran carreras universitarias sobre seguridad informática y uno de los objetivos es capacitar a los funcionarios que hacen parte de la ciberseguridad del país; también se crea el Centro Policial Cibernético - CCP, centrado más hacia la seguridad digital de la ciudadanía y determina que también está habilitado para dar capacitaciones sobre seguridad informática. Cada una de las medidas tomadas en este CONPES, ha sido funcional para la mitigación del *phishing*.

[73] Banco Interamericano de Desarrollo; Ministerio de Tecnologías de la Información y las Comunicaciones y Organización de los Estados Americanos. **Op. cit., p.79**

[74] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3854. Op. cit., p.12.

Sin embargo, como se puede observar cada grupo fue creado con un objetivo en común, la capacitación y sensibilización de los usuarios en general. Es indispensable tener como primera estrategia implementar campañas de sensibilización y capacitación a todos los usuarios, tanto a comunidad, como sector público y privado, buscando trabajar de la mano con cada sector. En el cuadro relacional de actividades concretas de este CONPES una de las más claras frente al tema de capacitación al sector privado y educación es el número 18. "Solicitar al Ministerio de Tecnologías de la Información y las Comunicaciones realizar las gestiones necesarias con el Ministerio de Educación Nacional y el SENA, para la generación de un plan de capacitación para el sector privado en temas de ciberseguridad y de seguridad de la información"[75].

El CONPES 3854 incluye la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital. Siendo su objetivo central fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital. Y propone que "en lugar de continuar tratando el riesgo de seguridad digital como un problema técnico que necesita soluciones técnicas, este también debería abordarse como un riesgo económico que debe gestionarse en cualquier proceso de toma de decisiones"[76]. Involucra activamente a todas las partes interesadas y hace énfasis especial en la responsabilidad compartida entre las mismas. "Colombia es el primer país de América Latina y uno de los primeros en el mundo en incorporar plenamente las recomendaciones y mejores prácticas internacionales en materia de gestión de riesgos y seguridad digital emitidas recientemente por la Organización para la Cooperación y el Desarrollo Económicos (OCDE)"[77].

Las 18 estrategias implementadas, de acuerdo con las mejores prácticas internaciones a groso modo, para llevar a buen término la política digital, fueron las siguientes:

- Establecer un marco institucional articulado que involucre a las múltiples partes interesadas para la implementación de la política nacional de seguridad digital.

- Implementar en el Gobierno nacional un modelo de gestión de riesgos de seguridad digital.

- Establecer mecanismos de participación activa y permanente de las múltiples partes interesadas en la gestión del riesgo de seguridad digital.

---

[75] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3701. Op. cit., p. 30.

[76] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3854. Op. cit., p.24.

[77] Banco Interamericano de Desarrollo; Ministerio de Tecnologías de la Información y las Comunicaciones y Organización de los Estados Americanos. **Op. cit.,** p. 100.

- Adecuar el marco legal y regulatorio en torno a la dinámica de la economía digital y sus incertidumbres inherentes.

- Identificar y abordar los posibles impactos negativos que otras políticas pueden generar sobre las actividades de las múltiples partes interesadas en el entorno digital o sobre la prosperidad económica y social.

- Generar confianza en las múltiples partes interesadas en el uso del entorno digital.

- Promover en los diferentes niveles de formación comportamientos responsables en el entorno digital.

- Fortalecer las instancias y entidades responsables de ciberseguridad.

- Adecuar el marco jurídico sobre los delitos cibernéticos, cibercrímenes y fenómenos en el entorno digital.

- Socializar y concientizar las tipologías de cibercrímen y ciberdelincuencia a las múltiples partes interesadas.

- Fortalecer las capacidades de los responsables de seguridad nacional en el ciberespacio y de la judicialización de delitos cibernéticos y cibercrímenes.

- Fortalecer las instancias y entidades responsables de la defensa nacional en el entorno digital.

- Adecuar el marco jurídico para abordar la protección y defensa del entorno digital nacional.

- Generar una estrategia de protección y defensa de la infraestructura crítica cibernética nacional.

- Fortalecer el esquema de identificación, prevención y gestión de incidentes digitales, con la participación activa de las múltiples partes interesadas.

- Fortalecer las capacidades de los responsables de garantizar la defensa nacional en el entorno digital.

- Generar mecanismos para impulsar la cooperación, colaboración y asistencia a nivel internacional, en materia de seguridad digital.

- Fortalecer la cooperación, colaboración y asistencia a nivel nacional, entre las múltiples partes interesadas en temas de seguridad digital.[78]

[78] CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3854. Op. cit., p. 24.

Cada una de las estrategias implementadas en esta política digital es necesaria para la mitigación del phishing y demás ataques informáticos ya que se centra en la gestión de riesgos. Según el CONPES 3854[79]. Este es el conjunto de actividades coordinadas, para abordar el riesgo digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones. Se basa en un conjunto flexible y sistemático de procesos cíclicos. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.

Las estrategias están diseñadas de tal forma que cada parte interesada note la importancia y la responsabilidad de su rol en ellas. Ya que, está basado en las mejores prácticas internaciones, que son totalmente funcionales para la comunidad, el sector privado y público, cada sector es importante para la economía y desarrollo digital del país y mediante estas estrategias se complementan y fortalecen armónicamente cada parte interesada y de esta manera es posible la mitigación no solo del *phishing* si no que de todos los ataques informáticos.

[79] Ibíd.,50.

7. ESTRATEGIAS DE SEGURIDAD DE LA INFORMACIÓN A TRAVÉS DE CONTROLES Y PRÁCTICAS PARA LA MITIGACIÓN DEL IMPACTO DE *PHISHING* EN LOS SECTORES MÁS ATACADOS POR ESTE DELITO INFORMÁTICO EN COLOMBIA DURANTE LOS ÚLTIMOS CINCO AÑOS.

Las estrategias propuestas se desarrollan tomando como base el CONPES 3854 Política Nacional De Seguridad Digital, ya que, fue realizada de acuerdo con las mejores prácticas internaciones, recomendadas por la OCDE que "incluyen la promoción de los principios generales sobre el conocimiento, las habilidades y la capacitación, la responsabilidad, los derechos humanos y los valores fundamentales, cooperación, evaluación de riesgos y ciclo de tratamiento, medidas de seguridad, de innovación y de preparación y continuidad"[80]. Estas estrategias implementadas en el CONPES 3854 articulan las múltiples partes interesadas, es decir los ciudadanos, sectores económicos y organizaciones y la norma ISO 27001 que es una norma internacional para implementar un Sistema de Gestión de la Seguridad de la Información, permitiendo así a las organizaciones evaluar el riesgo y la aplicar los controles necesarios para mitigarlos o eliminarlos.

7.1 ESTRATEGIAS PARA LA CUIDADANIA

El sector de la ciudadanía ha sido el sector con mayor impacto negativo por los ataques de phishing durante los últimos cinco años, por lo tanto, es necesario proponer estrategias efectivas que se puedan implementar en la vida cotidiana, las cuales le ayuden a tener seguridad en su información. Para ello se necesita el apoyo de las herramientas que ya ha generado el gobierno y algunas que podrían implementarse. Las estrategias se realizan frente a las vulnerabilidades identificadas.

- Estrategia 1 - Conocimiento: El Ministerio de educación de la mano con Ministerio de Tecnologías de la Información y Comunicaciones, deberían incluir clases de seguridad informática dentro de la materia de tecnología e informática que reciben hoy en día, adicionalmente realizar jornadas de educación sobre la seguridad informática, donde se involucre a los padres de familia y se capacite anualmente, en todos los colegios de Colombia, ya que, es de vital importancia que desde el inicio de la formación académica, los niños tengan herramientas de autoprotección digital. En la actualidad los niños desde la primaria infancia ya tienen celulares y conocimientos básicos en el manejo de equipos tecnológicos. En Colombia, "un estudio de la Fundación Telefónica reveló que el 42 por ciento de los niños de 6 a 9

[80] Banco Interamericano de Desarrollo; Ministerio de Tecnologías de la Información y las Comunicaciones y Organización de los Estados Americanos. Op. cit., p. 101.

años de edad tiene un celular"[81]. De esta manera se dan herramientas a los niños y adolescentes, para que puedan tener conocimientos básicos, como actualizar el sistema operativo, configurar el firewall, tener contraseñas seguras, entre otros. Estos conocimientos son trasmitidos a cada hogar y de esta manera se fortalece el conocimiento de seguridad informática y su importancia en la ciudadanía.

- Estrategia 2 – Inversión: Realizar diferentes campañas de sensibilización por todos los medios de comunicación, sobre los beneficios de obtener un antivirus legal como programa básico, para la seguridad del equipo tecnológico personal o del hogar y sobre las consecuencias de obtener programas piratas, en el mercado negro o páginas inseguras. Adicionalmente el gobierno debería dar facilidades a los estratos uno y dos para que puedan obtener un antivirus por hogar.

- Estrategia 3 – Buenas prácticas: Se propone a la ciudadanía seguir las siguientes recomendaciones generales de buenas prácticas de seguridad digital como: No dar información personal a desconocidos, por ningún medio; Cambiar periódicamente las contraseñas, no establecer una sola para los diferentes usos, crear contraseñas seguras que contenga números, letras mayúsculas, minúsculas y caracteres, utilizar sistema de doble autenticación. Frente a los correos electrónicos y mensajes de texto, no abrir enlaces desconocidos, no descargar documentos de destinarios que no conoce. En caso de necesitar actualizar datos personales diríjase a la página oficial de la entidad.

7.2 ESTRATEGIAS PARA LAS ORGANIZACIONES

Frente a las estrategias para las organizaciones más afectadas por los ataques de *phishing,* se propone implementar algunas estrategias de acuerdo con las vulnerabilidades identificadas.

- Estrategia 1 – Inversión: Se propone que el Gobierno Nacional de la mano con el Ministerio de hacienda, Ministerio de Tecnologías de la Información y Comunicaciones, la Superintendencia Financiera y entidades estatales que correspondan, otorguen facilidad y beneficios en las tasas de interés a los empresarios de pequeñas y medianas empresas, para inversiones específicas a la seguridad informática de sus empresas, impulsando de esta forma la implementación de herramientas y personal exclusivo en el área de seguridad informática. Asimismo, realizar publicidad por los medios de comunicación y con ayuda del colCERT realizar jornadas de capacitaciones en los diferentes sectores económicos, para crear conciencia de la importancia de invertir en el área de seguridad de la información y dando a conocer la política de seguridad digital del

[81] El tiempo. 24 de octubre de 2014. [Consultado 17 de octubre de 2020]. Disponible en https://www.eltiempo.com/archivo/documento/CMS-14751918

país, de esta forma los empresarios tendrán conciencia de la importancia de gestionar los riesgos de su organización y lo que se necesita para ello.

- Estrategia 2 – Personal: Es de vital importancia contratar personal idóneo, especializado en el área de seguridad informática, especialmente el jefe de área, ya que, es la persona que tiene la responsabilidad de realizar un diagnóstico sobre las necesidades de la organización y brindar mejor solución a gerencia.

- Estrategia 3 – Implementación de un Sistema de Gestión de Seguridad de la información: Implementar un SGSI que mejora la protección de los activos y permite gestionar el riesgo mediante aplicación de controles como lo recomiendan las mejores prácticas internacionales, como por ejemplo la norma ISO 27001, cuya estructura está definida por:

- Contexto de la organización: en ella propone para su implementación conocer las necesidades y expectativas de las partes interesadas de la organización, es decir los que puedan verse afectados por un riesgo de la empresa y asimismo determinar el alcance del SGSI.

- Liderazgo: La alta gerencia muestra su compromiso para llevar a cabo la implementación del SGSI asegurando los recursos necesarios, estableciendo una política de seguridad de la información junto con la asignación de roles y responsabilidades bien definidas de todas las partes interesadas. Como parte de la política de seguridad de la información establece las políticas para los dispositivos móviles, control de acceso, uso de controles criptográficos, de escritorio y pantalla limpios, de backups, procedimientos para la transferencia de información, desarrollo seguro y política de seguridad de la información para relaciones con proveedores.

- Planeación: Establecen las acciones para atender los riesgos y oportunidades, los objetivos de seguridad de la información y lo planes para alcanzarlos. Se realiza la evaluación de los riegos y su tratamiento

- Soporte: Dentro de ella se determinan los recursos, las competencias del personal, la conciencia sobre el rol y responsabilidad de estos, la comunicación de la organización sobre el SGSI. Se establece además que debe llevarse información documentada de los procesos de implementación y asimismo llevar un control documental.

- Operación: Se establece que la organización debe planear, implementar y controlar los procesos necesarios para cumplir los requisitos de seguridad.

- Evaluación de desempeño: Se define que se debe evaluar el desempeño de la seguridad de la información y la eficacia de SGSI, realizar auditorías internas y revisión por la dirección.

- Mejora: Realizar acciones correctivas frente a una no conformidad y mejorar de manera continua la idoneidad. Suficiencia y eficacia del SGSI[82].

los objetivos de control de la norma ISO 27001, se consideran de gran importancia para la mitigación del *phishing* ya que por medio de la aplicación de los 114 controles permite identificar los riesgos, tratarlos y gestionarlos. Dando una mayor seguridad a la información de las organizaciones. Se hace necesario destacar la importancia de la capación a las partes interesadas y la sensibilización a los usuarios dando conocer las políticas de seguridad implementadas en la organización y realizando un enfoque en la responsabilidad de cada rol, todas las partes interesadas deben ser conscientes de su papel con el fin de hacer frente a los riesgos de seguridad digital ya que las múltiples partes interesadas necesitan saber cómo afrontar las incertidumbres y reducir los riesgos.

7.3 OTROS CONTROLES Y BUENAS PRÁCTICAS

Adicionalmente se pueden realizan las siguientes recomendaciones, sobre controles y buenas prácticas para mitigar y prevenir, el impacto del *phishing* en Colombia:

- Bloquear contenido remoto en correos electrónicos: el contenido remoto hace referencia a partes de un mensaje, que no se ven a simple vista y no están incluidos realmente en el mensaje en sí, por ejemplo, imágenes; hojas de estilo o vídeos y al visualizar el correo electrónico, se descargan de internet, afectando la privacidad ya que, permite alertar al emisor del mensaje, dándole a conocer que se visualizó el correo electrónico y por lo tanto confirma que es una cuenta activa. Debido a esto es importante bloquear este contenido, evitando generar esta alerta que da información importante al ciberdelincuente e incrementa la probabilidad de caer en un ataque de *phishing*. Cada cliente de correo electrónico tiene una forma de bloquear este contenido.

- Identificar la dirección falsa del correo electrónico del remitente, generalmente suele ser incoherente, al no tener conexión con el contenido del mensaje, usa dominios desconocidos y se observa que proviene de otro país.

- La mayoría de los correos de *phishing*, hacen creer que proviene de bancos, solicitando actualización de datos o activación de servicios; entre otros. Por lo tanto, tener en cuenta que estos correos, cuando proviene de los bancos realmente suelen ser personalizados y contiene datos como nombre y apellido del cliente; últimos 4 dígitos de la cedula o últimos dígitos del número de la cuenta o tarjeta de crédito.

[82] ISOTOOLS. Norma ISO 27001:2013. [en línea]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/#

Por lo tanto, un correo *phishing*, llegará dirigiéndose de manera general, puede contener errores de ortografía. Adicionalmente, por políticas de privacidad de los bancos, no solicitan datos personales por este medio. En caso de ser necesario actualizar datos, se recomienda, dirigirse personalmente al banco; ingresar directamente a la página oficial o llamar al banco.

- Hacer uso de extensiones anti-*phishing*, como por ejemplo netcraft. Esta extensión permite identificar y bloquear páginas de *phishing* que se encuentran reportadas en diferentes partes del mundo. Por lo tanto, si el usuario por error da clic en el link de pesca, las extensiones anti-*phishing* generan la alerta informando que está ingresando a un sitio de *phishing* y será bloqueada.

- Estos correos normalmente contienen un link con nombre falso, para engañar al usuario, se dirige a la página que el ciberdelincuente desea finalmente, para robar datos. Es posible conocer el nombre real del link, al colocar la flecha sobre éste, se puede visualizar en la parte inferior de la página el nombre real del link. Realizar este paso es importante, antes de dar clic en un enlace sospechoso.

- Utilizar sistema de doble autenticación, por ejemplo, huella o utilizar un código que llegue al número de celular, para autorizar el acceso al correo.

- Habilitar el protocolo HTTPS en el navegador y no ingresar a páginas que no tengan el protocolo SSL.

- Establecer políticas de contraseñas seguras y del uso de dispositivos móviles.

- "Aprovechar las ventajas de la nube y tener redes segmentadas"[83].

- Utilizar protocolos de SPF, DKIM, DMARC, S / MIME y correo no deseado.

  El Sender Policy Framework, o SPF, es un estándar de autenticación que vincula un nombre de dominio a una dirección de correo electrónico. Consiste en definir cuál es el remitente (o remitentes) autorizado para enviar emails con un dominio determinado. De este modo, los clientes de emails como Gmail o Outlook pueden comprobar que el email entrante procede de un host autorizado por el administrador del dominio desde el que se envía.

  El DomainKeys Identified Mail, o DKIM, es un protocolo de autenticación que vincula un nombre de dominio a un mensaje. El protocolo te permite firmar tu email con tu nombre de dominio. El objetivo del protocolo DKIM no es sólo demostrar que el nombre

[83] DURAN, Sharon. 5 RECOMENDACIONES PARA EVITAR CIBERATAQUES EN TU EMPRESA. [en línea]. Enter.co. 2018. [Consultado: 10 de junio de 2018] Disponible en http://www.enter.co/especiales/empresas/5-recomendaciones-para-evitar-ciberataques-en-tu-empresa/

de dominio no ha sido usurpado, sino también que el mensaje no ha sido alterado durante la transmisión.

El Domain-based Message Authentication, Reporting and Conformance, o DMARC, es un estándar de autenticación que complementa a SPF y DKIM para combatir más eficazmente el phishing y otras prácticas de spamming. Permite a los propietarios de dominio indicar a los ISP (proveedores de servicios de Internet) y a los clientes de email qué hacer cuando un mensaje firmado de su dominio no está formalmente identificado por un estándar SPF o DKIM[84].

- "Gestión de certificados de, firma de correo electrónico"[85].

- "Implementar soluciones como anti-*phishing*; antivirus; antimalware, de filtrado de contenido y antispam de buena calidad en Internet, el análisis antivirus de puerta de enlace proporciona una capa adicional de defensa contra escaneo antivirus de escritorio"[86].

[84] REDONDO, Beatriz. SPF, DKIM y DMARC: Por qué usarlos y cómo configurarlos. [en línea]. Disponible en: https://es.mailjet.com/blog/news/spf-dkim-dmarc-como-configurar/

[85] PUBLICO, Ricky. ¿Qué es S/MIME y cómo funciona? [en línea]. GlobalSing. Marzo 2017. [Consultado: 26 de agosto de 2018]. Recuperado de https://www.globalsign.com/es/blog/que-es-smime/

[86] MCAFEE. Anti-Phishing: Best Practices for Institutions and Consumers. [En Línea] Recuperado: http://docs.apwg.org/sponsors_technical_papers/Anti-Phishing_Best_Practices_for_Institutions_Consumer0904.pdf

8. CONCLUSIONES

- Es importante mencionar que se clasificaron las diferentes modalidades de *phishing* utilizadas en Colombia frente a la concurrencia y finalidad de uso de los ciberdelincuentes. Identificando entre las modalidades principalmente, las siguientes: a. *Smishing,* se describe como el engaño realizado por mensaje de texto; b*. Vishing,* engaño por medio de llamadas; c. S*pear-phishing,* ataques dirigidos y d. *BEC,* ataque dirigido a gerencia. Entre las principales finalidades del *phishing* para los ciberdelincuentes, se encuentran realizar otros ciberataques, obtener un beneficio económico, o búsqueda de reconocimiento, incrementar su ego y mostrar el control y poder que tiene para mostrar sus habilidades cibernéticas ilegales, dañar la imagen del estado, ya que el ciberdelincuente puede tener fines políticos, como sabotajes en elecciones. Adicionalmente, ante ataques informáticos para un estado, buscan acceder a información confidencial, acceder abusivamente a los sistemas informáticos y muchos ataques se están centrando en la infraestructura crítica. Lo que se puede denominar ciberterrorismo, porque genera miedo, pone en riesgo la vida de las personas y afecta toda una población.

- Los ataques de *phishing* han impactado de una manera negativa la sociedad, afectando a las víctimas en el aspecto económico, psicológico, la confianza digital, el buen nombre de los usuarios, organizaciones y del estado. Durante el periodo estudiado, se encontró que el costo de perdidas denunciado oscilaba entre $300.000.000 y $5.000.000.000 para una estimación promedio de $2.350.000.000, demostrando que los ataques de *phishing* afectan cualquier tipo de empresa, abarcando desde las MiPymes, Pymes hasta las de grandes capitales.

- Se establecieron entre las vulnerabilidades más comunes de seguridad informática en dos grupos, el ciudadano y las organizaciones, siendo la principal vulnerabilidad del ciudadano el desconocimiento; como segunda vulnerabilidad se encuentra la falta de inversión en programas originales y apropiados; la tercera vulnerabilidad es la ausencia de buenas prácticas respecto a la seguridad informática. Frente a las vulnerabilidades más comunes de seguridad informática en las organizaciones, al igual que en los ciudadanos, la primera vulnerabilidad radica en que el nivel gerencial no invierte lo suficiente en herramientas y personal especializado en seguridad informática y la segunda vulnerabilidad es la ausencia de un sistema de gestión de seguridad de la información que conlleva a la creación de una política de seguridad de la información efectiva.

- Por otra parte, al identificar las estrategias y controles para la mitigación del *phishing* recomendadas en las políticas públicas relacionadas con la seguridad

informática en Colombia, el Gobierno nacional expidió el Documento CONPES 3701. Esta política concentró los esfuerzos del país en contrarrestar el incremento de las amenazas informáticas que lo afectaban significativamente, y en desarrollar un marco normativo e institucional para afrontar retos en aspectos de seguridad cibernética"[76]. Por otra parte, el CONPES 3854 en su política de seguridad digital, incluye la gestión de riesgo como uno de los elementos más importantes para abordar la seguridad digital, con el fin de fortalecer las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital.

- Finalmente, Colombia es el primer país de América Latina y uno de los primeros en el mundo en incorporar las recomendaciones y mejores prácticas internacionales en materia de gestión de riesgos y seguridad digital emitidas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE)", por lo tanto, se hace necesario proponer estrategias de seguridad de la información a través de controles y buenas prácticas para la mitigación del impacto de phishing en los sectores más atacados por este delito informático en Colombia durante los últimos cinco años.

9. RECOMENDACIONES

Se recomienda a la ciudadanía tomar responsabilidad frente a la seguridad de su información, aplicando buenas prácticas, como por ejemplo cambiar periódicamente las contraseñas, no anotarlas en ningún soporte físico o digital, no entregar información confidencial a personas que no conozca. Además, no descargar programas de páginas desconocidas, ni obtenerlos en el mercado negro. Asimismo, se recomienda realizar actualización permanente del sistema operativo, ya que esto brinda mayor seguridad ante las vulnerabilidades del sistema y utilizar antivirus.

Capacitar a los usuarios de la organización frente a la seguridad informática, los ataques informáticos especialmente el *phishing* y darle herramientas para que los usuarios tengan la habilidad de poder identificar un email de *phishing.* Para ello se necesita implementar campañas de sensibilización frente al problema en mención. Adicionalmente implementar en las empresas un Sistema de Gestión de Seguridad de la Información, asimismo realizar inversión en el área de Seguridad de la Información y asignar personal exclusivo e idóneo en al área.

Apoyarse en las instituciones creadas por el gobierno, para una respuesta a incidentes oportuna y eficiente. Además, para capacitaciones que sean necesarias para la organización y brindar capacitaciones especializadas en el área de seguridad informática al personal del área de seguridad de la información para mantener actualizados los conocimientos y hacerles frente a nuevos ataques informáticos que se puedan presentar.

BIBLIOGRAFÍA

AGUILERA, Purificación. Seguridad Informática [en línea]. Editex, 2010. 240 p. [Consultado: 11 de octubre de 2020]. Disponible en https://books.google.es/books?id=Mgvm3AYIT64C&dq=seguridad+inform%C3%A1tica&lr=lang_es&hl=es&source=gbs_navlinks_s

ANDREU, Fernando; PELLEJERO, Izaskun y LESTA Amaia. Fundamentos y Aplicaciones de Seguridad en Redes WLAN: Fundamentos y Aplicaciones de Seguridad. [en línea]. Marcombo, 2006. 160p. ISBN 8426714056, 9788426714053. [Consultado: 14 de octubre de 2020]. Disponible en https://books.google.com.co/books?id=k3JuVG2D9lMC&dq=que+es+spoofing&hl=es&source=gbs_navlinks_s

ASOSEC. El Phishing en Colombia. 2013. [En línea]. [Consultado: 5 de mayo de 2019]. Disponible en: http://asosec.co/2013/03/el-phishing-en-colombia/

BACA URBINA, Gabriel. Introducción a la Seguridad Informática [en línea]. México: Grupo editorial Patria, 2016. 331 p. [Consultado: 11 de octubre de 2020]. Disponible en: https://books.google.com.co/books?id=IhUhDgAAQBAJ&printsec=frontcover&dq=seguridad+informatica&hl=es&sa=X&ved=2ahUKEwiJv-PVgazsAhWMxFkKHQGICbkQ6AEwAHoECAMQAg#v=onepage&q&f=true ISBN: 978-607-744-471-8

Banco Interamericano de Desarrollo y Organización de los Estados Americanos, Op. cit., p. 6.

Banco Interamericano de Desarrollo y Organización de los Estados Americanos. Ciberseguridad Riesgos, Avances Y El Camino A Seguir En América Latina Y El Caribe [en línea]. BID. 2020. [Consultado: 16 de octubre de 2020]. Disponible en: https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/BID%20-%20OEA%20Reporte-Ciberseguridad-2020-riesgos-.pdf?ver=1601971104202

Banco Interamericano de Desarrollo; Ministerio de Tecnologías de la Información y las Comunicaciones y Organización de los Estados Americanos. Impacto de Los Incidentes de Seguridad Digital en Colombia 2017. [En línea]. [Consultado: 19 de

mayo de 2018]. Disponible en http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

Banco Interamericano de Desarrollo; Ministerio de Tecnologías de la Información y las Comunicaciones y Organización de los Estados Americanos. Op. cit., p. 101.

Banco Interamericano de Desarrollo; Ministerio de Tecnologías de la Información y las Comunicaciones y Organización de los Estados Americanos. Op. cit., p.60

Banco Interamericano de Desarrollo; Ministerio de Tecnologías de la Información y las Comunicaciones y Organización de los Estados Americanos. Op. cit., p. 100.

Banco Interamericano de Desarrollo; Ministerio de Tecnologías de la Información y las Comunicaciones y Organización de los Estados Americanos. Op. cit., p.79

BBC Mundo. 17 de diciembre de 2016. p.14 [consultado 15 de octubre de 2020]. Disponible en: https://www.bbc.com/mundo/noticias-internacional-38350244

BBVA, vishing. [En Línea]. [Consultado 20 de febrero de 2019]. Disponible en https://www.bbva.com/es/vishing-la-imaginacion-los-estafadores-no-limites/

BELCIC, Iván. ¿Qué es exactamente el phishing? [En Línea]. Avast. Agosto 2018 [Consultado: 20 de febrero de 2019]. Disponible en https://www.avast.com/es-es/c-phishing

BELISARIO MÉNDEZ, Aymara Noriley. Análisis de Métodos de Ataques de Phishing. Buenos Aires, 2014, 61 páginas. Trabajo de grado (Especialista). Universidad de Buenos Aires. Facultades de Ciencias Económicas, Cs. Exactas y Naturales e Ingeniería. [Consultado 12 de mayo de 2018] [En línea] Disponible en http://bibliotecadigital.econ.uba.ar/?c=tpos&a=d&d=1502-0840_BelisarioMendezAN

BENAVIDES, Eduardo, et al. Caracterización de Los Ataques de Phishing y Técnicas Para Mitigarlos. Ataques: Una Revisión Sistemática de La Literatura. [en línea]. Ciencia y Tecnología (1390-4051), vol. 13, no. 1, Jan. 2020, pp. 97–104. EBSCOhost, doi:10.18779/cyt.v13i1.357. [Consultado: 12 de octubre de 2020].

Disponible en: http://eds.b.ebscohost.com.bibliotecavirtual.unad.edu.co/eds/pdfviewer/pdfviewer?vid=1&sid=32b1d2c6-682a-4c86-86c7-c2fd65dc19ca%40pdc-v-sessmgr02

CARDOZO, Rossana. Atención al 'vishing': cómo detectarlo y protegerse. [en línea]. BBVA, 30 de agosto de 2019. [Consultado: 12 de octubre de 2020]. Disponible en: https://www.bbva.com/es/py/atencion-al-vishing-como-detectarlo-y-protegerse/

CENTRO CIBERNÉTICO POLICIAL: Capturado el "Rey de las millas [en línea]. [Consultado: 02 de julio de 2020] Disponible en: https://caivirtual.policia.gov.co/ciberseguridad/casos-operativos/capturado-el-rey-de-las-millas

CENTRO DE INVESTIGACIÓN DE DERECHO INFORMÁTICO – CIDI. [en línea]. Universidad Externado de Colombia. [Consultado: 11 de octubre de 2020]. Disponible en: https://www.uexternado.edu.co/centro-investigacion-derecho-informatico-cidi/

CENTRO DE INVESTIGACIÓN DE DERECHO INFORMÁTICO – CIDI. Objeto de Estudio, Óp. cit.

COLOMBIA, SECRETARÍA JURÍDICA DISTRITAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C. LEY 1273 DE 2009. [En línea]. [Consultado: 15 de junio de 2019] Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3701. (14, julio, 2011). Lineamientos de Política para Ciberseguridad y Ciberdefensa. [en línea]. [Consultado: 12 de mayo de 2019]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3854. (11, abril, 2016). Política Nacional de Seguridad Digital. [en línea]. [Consultado: 21 de agosto de 2019]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

COMANDO CONJUNTO CIBERNÉTICO. Misión y Responsabilidad. [En línea]. [Consultado: 21 de noviembre de 2017]. Disponible en https://www.ccoc.mil.co/quienes_somos/mision_responsabilidad

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3701. Op. cit., p. 30.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3701. Óp. cit., p. 9.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3854. Op. cit., p. 24.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3854. Op. cit., p.12.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3854. Op. cit., p.25.

CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3854. Op. cit., p.37.

DURAN, Sharon. 5 RECOMENDACIONES PARA EVITAR CIBERATAQUES EN TU EMPRESA. [en línea]. Enter.co. 2018. [Consultado: 10 de junio de 2018] Disponible en http://www.enter.co/especiales/empresas/5-recomendaciones-para-evitar-ciberataques-en-tu-empresa/

ECURED, Derecho Informático. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://www.ecured.cu/Derecho_inform%C3%A1tico

El Tiempo. 24 de octubre de 2014. [Consultado 17 de octubre de 2020]. Disponible en https://www.eltiempo.com/archivo/documento/CMS-14751918

El Tiempo. 26 de mayo de 2018. p. 7. [consultado 15 de octubre de 2020]. Disponible en: https://www.eltiempo.com/justicia/investigacion/ataques-a-pagina-web-de-la-registraduria-nacional-222756

ERB, Markus. Gestión de Riesgo en la Seguridad Informática. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://protejete.wordpress.com/about/

FISCALIA GENERAL DE LA NACIÓN. Datos abiertos de la Fiscalía General de la Nación. [en línea]. [Consultado: 15 agosto 2020]. Disponible en https://www.fiscalia.gov.co/colombia/gestion/estadisticas/

GABALDON, Luis Gerardo y PEREIRA Wilmer. Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico. En: DOSSIE. Porto Alegre. 2008. (27 p.) [Consultado: 14 de octubre de 2020]. Disponible en: https://www.scielo.br/pdf/soc/n20/a08n20.pdf

GOUJON, André. Phishing: Webmail, Redes Sociales Y Bancos Son Los Servicios Más Suplantados. [en línea]. Welivesecurity, enero de 2013. [Consultado 12 de mayo de 2018]. Disponible en: https://www.welivesecurity.com/la-es/2013/01/09/phishing-webmail-redes-sociales-bancos-servicios-mas-suplantados

Grupo de Respuesta a Emergencias Cibernéticas de Colombia ColCERT. Acerca de. [En línea]. Julio de 2017. [Consultado: 12 de julio de 2018]. Disponible en http://www.colcert.gov.co/?q=acerca-de
Ibíd., p. Informática.

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

ISOTOOLS. Norma ISO 27001:2013. [en línea]. Disponible en: https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/#

KALI. Acerca de Kali Linux. [en línea]. [Consultado 12 de octubre de 2020]. Disponible en: https://www.kali.org/about-us/

LUBECK, Luis. Phishing suplanta identidad de reconocido banco de Colombia y busca robar información financiera. En: Welivesecurity: Campaña de phishing activa dirigida a usuarios de Colombia suplanta identidad de reconocido banco con el objetivo de robar credenciales de acceso y datos de las tarjetas de crédito y débito [en línea] Junio, 2019. [Consultado: 14/08/2020]. Disponible en https://www.welivesecurity.com/la-es/2019/06/05/phishing-activo-reconocido-banco-colombia/

MAESTROS DEL WEB, Tabnabbing. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en http://www.maestrosdelweb.com/que-es-tabnabbing-phishing-robo-identidad/

MALWAREBYTES. Software malicioso. [en línea]. [Consultado 13 de octubre de 2020]. Disponible en https://www.malwarebytes.com/malware/

MALWAREBYTES. Suplantación de identidad: (phishing). [en línea]. [Consultado: 10 de octubre de 2020] Disponible en https://es.malwarebytes.com/phishing/#:~:text=Suplantaci%C3%B3n%20de%20identidad%20(phishing),correo%20electr%C3%B3nico%20o%20llamada%20telef%C3%B3nica.

MARTÍNEZ, Carlos, et al. Seguridad por capas frenar ataques de Smishing. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en Dialnetdialnet.unirioja.es

MCAFEE. Anti-Phishing: Best Practices for Institutions and Consumers. [En Línea] Recuperado: http://docs.apwg.org/sponsors_technical_papers/Anti-Phishing_Best_Practices_for_Institutions_Consumer0904.pdf

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. [en línea]. Madrid, Subdirección General de

Información, Documentación y Publicaciones Jesús González Barroso, octubre de 2012. 127 p. [Consultado: 11 de octubre de 2020]. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html NIPO: 630-12-171-8

MOPOSITA GUANGASHI, Paul Fernando. “Medidas de protección informática para evitar el robo de identidad provocado por el ataque phishing “the Tabnabbing attack" para la facultad de ingeniería en sistemas, electrónica e industrial”. Ecuador, 2012, 176 páginas. Trabajo de grado (Ingeniero en Sistemas Computacionales e Informáticos.). Universidad técnica de Ambato. Facultad de ingeniería en sistemas, electrónica e industrial carrera de ingeniería en sistemas computacionales e informáticos. [En línea]. [Consultado: 19 de marzo de 2019]. Disponible en: http://repositorio.uta.edu.ec/handle/123456789/2378

MUÑOZ, José Manuel. La evaluación psicológica forense del daño psíquico: propuesta de un protocolo de actuación pericial. En: Redalyc. [en línea]. Red de Revistas Científicas de América Latina, el Caribe, España y Portugal. Madrid, España. vol. 23, 2013, pp. 61-69. [Consultado: 16 de octubre de 2020]. Disponible en https://www.redalyc.org/pdf/3150/315028685010.pdf ISSN 1133-0740.

Ola de ataques informáticos en todo el mundo. En: revista Semana. [en línea]. Diciembre de 2017. [Consultado: 23 de octubre de 2018]. Disponible en: https://pruebas.semana.com/tecnologia/articulo/ola-de-ataques-informaticos-en-todo-el-mundo/524914

PANDA. ‘Whaling’, el nuevo fraude que amenaza a tu empresa. 2016. [En línea]. (junio de 2016). [Consultado: 19 de marzo de 2019]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/whaling-amenaza-contra-empresas/

PANDA. 10 consejos Para Evitar Ataques De Phishing. [En línea]. Febrero de 2016. [Consultado:12 de mayo de 2018]. Disponible en https://www.pandasecurity.com/spain/mediacenter/consejos/10-consejos-para-evitar-ataques-de-phishing/

PANDA. En la cabeza del cibercriminal: ¿qué busca y por qué quiere atacar tu empresa? 2015. [En línea]. [Consultado 5 de mayo de 2019]. Disponible en: https://www.pandasecurity.com/spain/mediacenter/seguridad/en-la-cabeza-del-cibercriminal-que-busca-y-por-que-quiere-atacar-tu-empresa/

PASTORINO, Cecilia. Convenio de Budapest: beneficios e implicaciones para la seguridad informática. [En línea]. WELIVESECURITY. Diciembre de 2017. [Consultado: 06 de diciembre de 2017]. Disponible en https://www.welivesecurity.com/la-es/2017/12/06/convenio-budapest-beneficios-implicaciones-seguridad-informatica/

PÉREZ, J. C. Protección de datos y seguridad de la información: guía práctica para ciudadanos y empresas (4a. ed.). [en línea]. RA-MA Editorial. 2015. 277 p. [Consultado: 11 de octubre de 2020]. Disponible en: https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/106483?page=1 ISBN: 9788499645919

PETER, Nyheim, Estrategias tecnológicas para la industria de la hostelería. [en línea]. Ediciones Universidad Católica de Salta, 2019. 276 p. ISBN 9506231818. [Consultado 14 de octubre de 2020]. Disponible en: https://books.google.com.co/books?id=TmK4DwAAQBAJ&dq=Ataque+DDOS&hl=es&source=gbs_navlinks_s

PLAZAS GARCIA, Edna Roció. Ingeniería Social en las Empresas Colombianas. [En línea]. Pitalito, 2018, 75 Pág. Monografía. Universidad Nacional Abierta y a Distancia UNAD. Escuela de Ciencias Básicas, Tecnología e Ingeniería. Especialización en Seguridad Informática. [Consulado: 10 de noviembre de 2019]. Disponible en: https://stadium.unad.edu.co/preview/UNAD.php?url=/bitstream/10596/18704/1/1094921881.pdf

POLICIA NACIONAL y CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES, Óp. cit., p. 8.

POLICIA NACIONAL y CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias Cibercrimen Colombia 2019-2020 [en línea]. Bogotá. Octubre 29 del 2019. 36 páginas. Primera edición [Consultado: 12 de julio de 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

POLICIA NACIONAL. Amenazas del Cibercrimen en Colombia 2016-2017. [En línea]. [Consultado 5 de mayo de 2019]. Disponible en:

https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

POLICIA NACIONAL. Balance Cibercrimen en Colombia 2017. Colombia, 2017, Pág. 3 [en línea]. [Consultado: 19 de marzo de 2019] Disponible en: https://caivirtual.policia.gov.co/contenido/informe-balance-del-cibercrimen-2017

POSADA MAYA, Ricardo. Los cibercrímenes: Un nuevo paradigma de criminalidad. Un estudio del título VII bis del Código Penal colombiano. [en línea]. Bogotá: Grupo Editorial Ibáñez, 2017. 484 p. [Consultado: 11 de octubre de 2020]. Disponible en https://elibro-net.bibliotecavirtual.unad.edu.co/es/ereader/unad/118331?page=7 ISBN 9789587498141

PROOFPOINT, State of the Phish [en línea]. 2020. [Consultado: 07 de octubre de 2020]. Disponible en: https://www.proofpoint.com/sites/default/files/2020-06/pfpt-es-state-of-the-phish-2020-reports-a4.pdf

PUBLICO, Ricky. ¿Qué es S/MIME y cómo funciona? [en línea]. GlobalSing. Marzo 2017. [Consultado: 26 de agosto de 2018]. Recuperado de https://www.globalsign.com/es/blog/que-es-smime/

QUIROZ, Jhon Henry y FORERO CRUZ, William. Diseño de Recomendaciones de Seguridad Informática sobre los Activos de Información Críticos de la Empresa Gran Tierra Energy Colombia - Seccional Bogotá. [En Línea]. [Consultado 20 de febrero de 2019]. Disponible en repository.ucatolica.edu.co

RAE, Internet. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://dle.rae.es/?id=LvskgUG

RAE: Telecomunicación. óp. cit.,

REDONDO, Beatriz. SPF, DKIM y DMARC: Por qué usarlos y cómo configurarlos. [en línea]. Disponible en: https://es.mailjet.com/blog/news/spf-dkim-dmarc-como-configurar/

RODRÍGUEZ PUENTES, Marcos. Responsabilidad bancaria frente al phishing. [En línea]. Bogotá, 2015,102 Pág. Monografía. Universidad Nacional de Colombia.

Facultad de Derecho, Ciencias Políticas y Sociales. Departamento de Derecho. [Consulado: 10 de noviembre de 2019]. Recuperado de http://bdigital.unal.edu.co/53188/1/marcosrodriguezpuentes.2015.pdf

RUIZ ALONSO, Luis Alejandro. Diseño de Modelo de Seguridad Informática Basado en la Gestión de Incidentes para el área de Sistemas y Tecnología de Abril Publicidad en Bogotá Colombia. [En línea]. Bogotá, 2014, 86 Pág. Monografía. Universidad Piloto de Colombia, Facultad de Posgrados, Especialización en Seguridad Informática. [Consulado: 10 de noviembre de 2019]. Recuperado de http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2976/00001518.pdf?sequence=1&isAllowed=y

S21sec, Spear phishing. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://www.s21sec.com/es/blog/2013/05/glosario-de-terminos-que-es-el-spear-phishing/

SD, Alberto. Kaspersky registra 45 ataques por segundo en América Latina [en línea]. KASPERSKY. 2019. [Consultado: 07 de octubre de 2020]. Disponible en: https://latam.kaspersky.com/blog/kaspersky-registra-45-ataques-por-segundo-en-america-latina/15274/

SECURELIST. El Spam y el phishing en 2018. [En línea]. [Consultado: 5 de mayo de 2019]. Disponible en https://securelist.lat/spam-and-phishing-in-q1-2018/86992/

SECURIZANDO, Whaling. [En Línea]; [Consultado: 20 de febrero de 2019]. Disponible en https://securizando.com/whaling/

SEGU.INFO, Phishing. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://www.segu-info.com.ar/malware/phishing.htm

TÉLLEZ VALDÉS, Julio. Contratos Informáticos. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://books.google.com.co/books?id=m-MwmFPGCxQC&pg=PA33&dq=QUE+ES+riesgo+informatico&hl=es-419&sa=X&ved=0ahUKEwjQ2tOx9JPgAhXpY98KHUP8AKgQ6AEIKDAA#v=onepage&q=QUE%20ES%20riesgo%20informatico&f=false

The Open Web Application Security Project – OWASP. Ingeniería Social. [en línea]. República Dominicana. OWASP LatamTour, 2016. [Consultado 12 de octubre de 2020]. Disponible en: https://owasp.org/www-pdf-archive/02_INGENIER%C3%8DA_SOCIAL.pdf

UNIVERSIDAD NACIONAL DE LUJAN, Departamento de seguridad informática: Activo de Información. [En Línea]. [Consultado: 19 de febrero de 2019]. Disponible en http://www.seguridadinformatica.unlu.edu.ar/?q=taxonomy/term/22

UNIVERSIDAD NACIONAL DE LUJAN, Departamento de seguridad informática: Amenaza. óp. cit.,

UNIVERSIDAD NACIONAL DE LUJAN, Departamento de seguridad informática: Confidencialidad. óp. cit.,

UNIVERSIDAD NACIONAL DE LUJAN, Departamento de seguridad informática: Disponibilidad. óp. cit.,

VÁSQUEZ, Magaly y CHACÓN, Nelson. Ciencias penales, Citado por: JIJENA LEIVA, Renato Javier. La criminalidad Informática. [En Línea]. [Consultado: 20 de febrero de 2019]. Disponible en https://books.google.com.co/books?id=-jVch6LUPaQC&pg=PA582&dq=definici%C3%B3n+delito+informatico&hl=es&sa=X&ved=0ahUKEwi3r9Xl7MrgAhVrw1kKHX82DToQ6AEILjAB#v=onepage&q=definici%C3%B3n%20delito%20informatico&f=false

ANEXOS

ANEXO I. Resumen Analítico en Educación - RAE

Fecha de Realización:	20/10/2020
Programa:	Especialización en Seguridad Informática
Línea de Investigación:	Infraestructura tecnológica y seguridad en redes
Título:	Estudio Monográfico: Impacto De La Técnica De Ataque De Phishing En Colombia Durante Los Últimos Cinco Años
Autor(es):	Rueda Quintero Jeniffer Andrea
Palabras Claves:	phishing, delitos informáticos, seguridad informática, gestión de riesgos, capacitación a usuarios.
Descripción:	En la monografía se logró establecer la modalidad, finalidad y concurrencia con que los delincuentes informáticos utilizan las técnicas de phishing, adicionalmente se da a conocer el impacto social y económico que ha causado los ataques de phishing, durante los últimos cinco años en Colombia. Asimismo, se identificó los sectores con más denuncias por ataques informáticos junto con las vulnerabilidades más comunes, en los sectores con mayor afectación, seguidamente se da a conocer las estrategias implementadas por el Gobierno Nacional, haciendo énfasis en los CONPES 3701 Y 3854 donde se encuentra la política de seguridad digital, cuyas estrategias están basadas en las mejores prácticas internacionales, enfocadas en la gestión de riesgos. Con base en la identificación de las vulnerabilidades en los sectores más afectados por los ataques informáticos y en la política de seguridad digital, la norma ISO 27001, basada en un Sistema de Gestión de Seguridad de la Información y las recomendaciones

	internacionales, se proponen estrategias que ayuden a mitigar el phishing en Colombia. En cuanto a la ciudadanía, ofrecer conocimientos básicos sobre la seguridad de la información desde los colegios, e involucrar a los padres de familia en jornadas de capacitaciones y crear sensibilización y conciencia por los medios de comunicación sobre la importancia de la seguridad informática. Frente a las organizaciones se propone crear facilidades para que las pequeñas y medianas empresas puedan acceder a créditos con tasas preferenciales, para inversión en seguridad digital y apoyarse de los grupos creados como colCERT para brindar capacitaciones sobre la gestión de riesgos

Fuentes bibliográficas destacadas:

Banco Interamericano de Desarrollo y Organización de los Estados Americanos. Ciberseguridad Riesgos, Avances Y El Camino A Seguir En América Latina Y El Caribe [en línea]. BID. 2020. [Consultado: 16 de octubre de 2020]. Disponible en: https://img1.wsimg.com/blobby/go/b653c9ee-535c-4528-a9c5-bb00166ad0dc/downloads/BID%20-%20OEA%20Reporte-Ciberseguridad-2020-riesgos-.pdf?ver=1601971104202

Banco Interamericano de Desarrollo; Ministerio de Tecnologías de la Información y las Comunicaciones y Organización de los Estados Americanos. Impacto de Los Incidentes de Seguridad Digital en Colombia 2017. [En línea]. [Consultado: 19 de mayo de 2018]. Disponible en http://www.oas.org/documents/spa/press/Estudio-Seguridad-Digital-Colombia.pdf

COLOMBIA, SECRETARÍA JURÍDICA DISTRITAL DE LA ALCALDÍA MAYOR DE BOGOTÁ D.C. LEY 1273 DE 2009. [En línea]. [Consultado: 15 de junio de 2019] Disponible en http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=34492

COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3701. (14, julio, 2011). Lineamientos de Política para Ciberseguridad y Ciberdefensa. [en línea]. [Consultado: 12 de mayo de 2019]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3701.pdf

COLOMBIA. CONSEJO NACIONAL DE POLÍTICA ECONÓMICA Y SOCIAL, et al. CONPES 3854. (11, abril, 2016). Política Nacional de Seguridad Digital. [en línea]. [Consultado: 21 de agosto de 2019]. Disponible en: https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf

FISCALIA GENERAL DE LA NACIÓN. Datos abiertos de la Fiscalía General de la Nación. [en línea]. [Consultado: 15 agosto 2020]. Disponible en https://www.fiscalia.gov.co/colombia/gestion/estadisticas/

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/No rma.%20NTC-ISO-IEC%2027001.pdf

MINISTERIO DE HACIENDA Y ADMINISTRACIONES PÚBLICAS. MAGERIT – versión 3.0: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I – Método. [en línea]. Madrid, Subdirección General de Información, Documentación y Publicaciones Jesús González Barroso, octubre de 2012. 127 p. [Consultado: 11 de octubre de 2020]. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html NIPO: 630-12-171-8

POLICIA NACIONAL y CÁMARA COLOMBIANA DE INFORMÁTICA Y TELECOMUNICACIONES. Tendencias Cibercrimen Colombia 2019-2020 [en línea]. Bogotá. Octubre 29 del 2019. 36 páginas. Primera edición [Consultado: 12 de julio de 2020]. Disponible en: https://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

POLICIA NACIONAL. Amenazas del Cibercrimen en Colombia 2016-2017. [En línea]. [Consultado 5 de mayo de 2019]. Disponible en: https://caivirtual.policia.gov.co/sites/default/files/informe_amenazas_de_cibercrimen_en_colombia_2016_-_2017.pdf

POLICIA NACIONAL. Balance Cibercrimen en Colombia 2017. Colombia, 2017, Pág. 3 [en línea]. [Consultado: 19 de marzo de 2019] Disponible en: https://caivirtual.policia.gov.co/contenido/informe-balance-del-cibercrimen-2017

Contenido del documento:	El contenido de esta monografía consta de las siguientes partes: • Definición del problema: ¿Cuál ha sido el impacto del phishing en términos sociales y

	económicos en Colombia durante los últimos cinco años? Y ¿Cuáles estrategias de seguridad de la información se recomiendan para la mitigación del impacto del phishing en el país? • Justificación: Muestra la importancia de realizar acciones para la mitigación del *phishing*. • Objetivo General: Proponer estrategias de seguridad de la información a través de controles y buenas prácticas para la mitigación del impacto de phishing en los sectores más atacados por este delito informático en Colombia durante los últimos cinco años. • Objetivos Específicos: 1. Clasificar las modalidades de phishing utilizadas en Colombia frente a la concurrencia y finalidad de uso de los ciberdelincuentes. 2. Identificar el impacto económico y social del phishing en los sectores con mayores denuncias en Colombia durante los últimos cinco años. 3. Establecer las vulnerabilidades más comunes de seguridad de la información en los sectores con mayores denuncias en Colombia durante los últimos cinco años. 4. Identificar las estrategias y controles para la mitigación del phishing recomendadas en las políticas públicas relacionadas con la seguridad informática en Colombia. • Delimitación: Se realiza la especificación del alcance de esta monografía como proyecto de grado. • Marco Referencial: el marco referencial está compuesto por los antecedentes que es donde

	muestran monografías complementarias para el trabajo de grado ya que hacen mención de el objeto de estudio. Seguidamente está el marco teórico, allí se abordan los temas que son importantes para el desarrollo del trabajo de grado, empezando de los temas más generales a los más específicos y se muestran algunas teorías establecidas. Después se realiza el desarrollo del marco conceptual, donde se da a conocer y se especifica sobre los conceptos más importantes para el desarrollo de esta monografía. En el marco histórico se da a conocer los avances del phishing desde sus principios hasta el tiempo actual y culmina con el marco legal que es la base jurídica colombiana sobre lo respectivo a la seguridad de la información y delitos informáticos. • Resultados Como resultado se obtiene la clasificación de las modalidades de phishing frente a la concurrencia y finalidad de los ciberdelincuentes, adicionalmente se muestra el impacto social y económico del phishing en Colombia durante los últimos cinco años. En consecuencia, se identifican las principales vulnerabilidades de seguridad informática en los sectores con mayores denuncias por ataques informáticos en Colombia y asimismo se identifica que las estrategias implementadas en el CONPES 3854 Política de seguridad digital, al tener un énfasis en la gestión del riesgo, involucrando las partes interesadas y siguiendo las recomendaciones internaciones, ayuda a mitigar el phishing en Colombia Finalmente se proponen algunas estrategias para la ciudadanía y las organizaciones con la finalidad de mitigar el phishing en Colombia. Conclusiones y recomendaciones generales.

Marco Metodológico:	Para el desarrollo de esta monografía se implementaron las siguientes fases: PLANEACIÓN: Recolección de información. Clasificación de Información. Análisis de la información más relevante. EJECUCIÓN: Desarrollo de objetivos Clasificación de métodos de phishing Muestra de Impacto de phishing en Colombia Identificación de vulnerabilidades Análisis de resultado de las estrategias de la política de seguridad digital RESULTADO: Propuesta de estrategias, teniendo en cuenta las vulnerabilidades identificadas y con base en los CONPES y en el Sistema de Gestión de Seguridad de la información norma ISO 27001
Conceptos adquiridos:	Se adquiere conocimientos como, las nuevas técnicas de phishing, los diferentes vectores de ataque y finalidades de uso por parte de los ciberdelincuentes, se dimensiona con más claridad el daño causado y se prevé el daño que puede causar con base en los datos analizados. Se toma conciencia de la importancia de realizar buenas practicas frente a la seguridad de la información y se aprenden herramientas básicas para a mitigación del phishing. Se obtiene aprendizaje sobre la gestión de riesgos su importancia.

Conclusiones:	En los últimos cinco años, los tres ataques más utilizados por los ciberdelincuentes en Colombia fueron el malware con 6.017 casos, la suplantación de identidad, en el segundo lugar, con 5.412 casos, en tercer lugar, se encuentra el phishing con 5.371 casos reportados. Por último, en los últimos lugares se ubicaron la ingeniería social con 875 reportes, el Spoofing con 657 casos y el ataque DDOS en el último puesto con 292 reportes con un promedio anual de 58 casos siendo la modalidad con menor incidencia. Colombia ha venido desarrollando diferentes estrategias, políticas y normatividad para la ciberseguridad y ciberdefensa del país, fortaleciendo las instituciones del gobierno, apoyando al sector privado y al usuario del común. Sin embargo, el avance de los ataques informáticos llega más allá de los esfuerzos realizados y han impactado de forma negativa esta confianza digital en los usuarios y organizaciones del país. En los últimos cinco años 74.645 usuarios en Colombia, fueron víctimas de ataques informáticos, en promedio 14.929 víctimas por cada año, siendo las ciudades más afectadas, Bogotá con 5.308 casos, seguido por Medellín y Cali. El sector más afectado es el ciudadano con un reporte total en los últimos cinco años de 30.689 denuncias; en segundo lugar, el sector financiero con total de 5.643 del año 2015 al 2019 en tercer lugar está el sector de la educación, con un total de reportes de 2.718. Los tres sectores con menos denuncias fueron el sector gobierno, los medios de comunicación y el sector salud. Los ataques de phishing han impactado de una manera negativa la sociedad, afectando a las víctimas en el aspecto psicológico, la confianza digital, el buen nombre de los usuarios, organizaciones y del estado. Durante el periodo estudiado, se encontró que el costo

	denunciado oscilaba entre $300.000.000 y $ 5.000.000.000 para una estimación promedio de $2.350.000.000, demostrando que los ataques de phishing afectan cualquier tipo de empresa, abarcando desde las MiPymes, Pymes hasta las de grandes capitales.