XX Congreso Internacional de Análisis Organizacional (XX CIAO)
"Fenómenos organizacionales emergentes en Latinoamérica frente a la crisis global: Homenaje a Guillermo Ramírez Martínez, 20 años realizando el CIAO"

Phishing en las Organizaciones, un Análisis más allá de lo Económico

Mesa Temática: Enfoques metodológicos para el análisis organizacional

Modalidad de la ponencia: Protocolo de Investigación

Marta Cecilia Sepúlveda Osorio[1]
ORCID: https://orcid.org/0000-0002-1992-4305
Colombiana
Correo Electrónico: marthace0224@hotmail.com

Universidad Autónoma Metropolitana
Av. San Rafael Atlixco 186, Leyes de Reforma 1ra Secc. Iztapalapa, 09340 Ciudad de México, CDMX, México
09040/Ciudad de México/México

Cartagena de Indias, Bolívar, Colombia, del 3 al 7 de octubre de 2022

[1] Autor responsable de la comunicación

Phishing en las Organizaciones, un Análisis más allá de lo Económico

Resumen

El phishing es un fenómeno que permea en toda la sociedad y ha venido en aumento exponencial a nivel mundial, afectando no solo grandes organizaciones, sino también personas externas a la organización, generando repercusiones a nivel económico y social. Dicho fenómeno replantea la forma como las organizaciones deben seleccionar a sus colaboradores, debido a que, las acciones del phishing afectan las organizaciones a nivel interno y externo, generando graves consecuencias al Good Will que conlleva a pérdidas irreversibles del público objetivo.
Mucho se ha investigado sobre las afectaciones monetarias que genera el phishing, pero poco sobre el factor humano y los factores que conllevan al individuo, bien sea interno o externo a la organización a cometer un fraude electrónico como el phishing, por lo cual se plantea como objetivo describir los factores sociales por los cuales el empleado de una organización decide realizar un phishing.

Palabras clave: fraude**,** factores sociales**,** colaborador, cibercrimen.

Introducción

El auge tecnológico corresponde a uno de los fenómenos más importantes a lo largo de la historia, el impacto que ha generado en la sociedad ha dado lugar a grandes transformaciones desde el ámbito económico, social, cultural y político, permitiendo alcanzar avances que han contribuido al progreso del mundo y la humanidad, ofreciendo la facilidad para realizar actividades y llevar a cabo procesos que anteriormente se dificultaban y requerían de un largo período de tiempo para ejecutarse con éxito; pese a los beneficios, la era informática considerada hoy en día como la cuarta revolución industrial, proveniente de la industria 4.0, donde las organizaciones junto con las transformaciones digitales de la industria y la incorporación de herramientas como Big data, internet de las cosas, la nube, ciberseguridad se enmarcan en ciudades inteligentes (Joyanes, 2017).

Lo anterior, ha creado un nuevo nicho para albergar delitos que se volvieron mundiales dando como resultado un cibercrimen, el cual, por medio de dichos avances, continúa desarrollando nuevas formas y estrategias para cometer violaciones y fraudes informáticos de modo que su detección cada vez se haga más difícil.

Dada la globalización, la tecnología ha avanzado enormemente, y con ella el incremento de los delitos electrónicos o cibercrimen; ataques que ponen en riesgo la economía personal y organizacional según el caso. Asimismo, tanto las personas como las organizaciones se encuentran constantemente expuestas al riesgo de ser víctimas de fraude electrónico, por lo tanto, de acuerdo a lo indicado por Domínguez (2018) ninguna

organización se encuentra exenta a estos delitos, en especial al phishing, y a pesar que se ha investigado sobre el cibercrimen y las formas de contraatacarlo o prevenirlo, poco sobre los motivos que conllevan a las personas a realizar un delito de tal magnitud.

Ante el anterior panorama, se enfatizará en el phishing, modalidad del fraude electrónico, específicamente en su concepto, origen e historia, estructura, tipos de phishing, phishing en las organizaciones, análisis desde las perspectivas interpretativa y prospectiva, así como algunos factores que influyen en la persona que realiza el fraude. Cabe mencionar que el 95% de los casos concernientes a la seguridad, están relacionados con algún error humano (Giraldo y Duarte, 2018).

Descripción del Problema

Actualmente existen diversas investigaciones sobre la afectación o consecuencias de los fraudes electrónicos, entre las cuales se encuentran: Gabaldón y Pereira (2008) en la investigación titulada “usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico” indican que se debe poner especial atención a los fraudes cometidos virtualmente, dado que sus consecuencias sobrepasan los daños económicos, y finaliza reflexionando acerca del balance que debe conservarse entre mecanismos de seguridad y la carga adicional generada a usuarios por la cantidad de formas de validaciones en transacciones electrónicas; al tiempo que recalca la necesidad de enfocarse en oportunidades delictivas, que brindan mayor entendimiento y reducción de esta clase de fraude.

Otra investigación correspondiente al “fraude electrónico desde el contexto jurídico venezolano” de Pacheco (2022), plantea por objetivo analizar la evolución del fraude, así como el impacto de la regulación legal que se presenta en Venezuela sobre la afectación que genera el fraude en las personas y concluye que son delitos a los cuales se les debe poner la lupa, con el fin de prevenir enormes consecuencias generadas a nivel de privacidad y datos. Finalmente, la investigación realizada por Ruiz (2021) llamada “fraude en el sector asegurador por medios electrónicos”, menciona que el fraude en compañías financieras por lo general involucra personas con algún vínculo en la organización, y lo mismo ocurre con las aseguradoras, sin embargo, con la emergencia generada con el covid-19 aumentan exponencialmente estos fraudes por pocos controles, asimismo, se centra en la importancia de producir estrategias encaminadas a la

disminución de riesgos presentados por el fraude electrónico en compañías aseguradoras.

Sin embargo, pocos se han interesado en describir y asociar el comportamiento y/o motivos que conllevan o se derivan de estos, y justamente en este último punto, se evidencia una anomalía, de acuerdo con Kuhn (Solís, 2010), porque normalmente se ha estudiado los efectos que produce el fraude electrónico en las personas y empresas, más no en conocer lo que motiva al ser humano realizar dicho fraude, para desde allí tomar medidas que brinden la protección necesaria a las organizaciones; parece mayor el interés en los daños económicos y formas de evitar el fraude electrónico tanto en personas como en organizaciones, que el estudio del comportamiento humano, como uno de los actores de la organización; de allí la importancia de ir más allá de lo económico. El anterior panorama genera una crisis que conlleva a una revolución, en la medida en que se crea un nuevo paradigma, que antes no estaba contemplado socialmente.

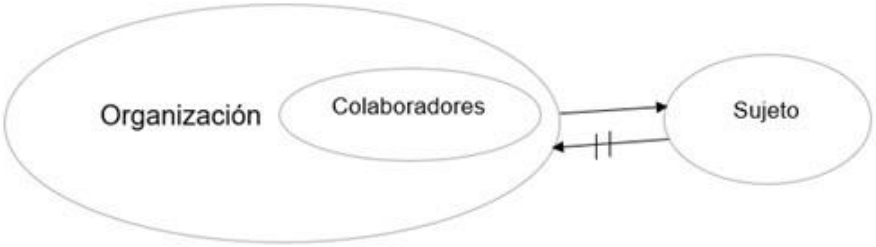
Teniendo en cuenta los factores asociados a las razones por las cuales el individuo toma la decisión de realizar un fraude electrónico a una organización, la teoría de las relaciones humanas tiene al ser humano como eje central de la organización, a diferencia de la teoría clásica que lo concibe como una máquina en busca de incrementar la productividad. Uno de los colaboradores de Elton Mayo, Frederick Herzberg propone la teoría de los dos factores, donde la satisfacción se asocia con la motivación, y la insatisfacción con la higiene, dentro de los factores de higiene se encuentran: salario, política de la empresa, relaciones interpersonales, entre otros (también llamados extrínsecos, al encontrarse fuera o externamente del individuo); algunos factores de motivación son: logros, reconocimientos, independencia laboral, entre otros (conocidos como intrínsecos,

al estar dentro del colaborador), manifiesta que la motivación del ser humano se presenta por factores intrínsecos, no extrínsecos (Martínez, 2013).

Se ha evidenciado que a nivel mundial diferentes organizaciones han protagonizado fraudes virtuales donde se ven comprometidos sus capitales y usuarios. A pesar que algunas de estas han fortalecido su sistema de protección ante delitos electrónicos, no es suficiente para lograr una protección completa; de acuerdo con el reporte de la revista Semana (2021), el ciberdelito en los últimos 3 años es una de las tipologías criminales de mayor crecimiento en Colombia. Al respecto reviste importancia esto, dado que se pretende describir los factores asociados que influyen en el comportamiento del sujeto que comete el fraude, el cual puede ser colaborador de la organización, que, motivado por insatisfacción, decide realizar el fraude, o un sujeto externo a la organización, diferente al colaborador, que motivado por el entorno toma la decisión de realizar el fraude, como se observa en la Figura 1.

Figura 1

Relación entre actores que participan en un fraude electrónico



Nota. Elaboración propia.

Este planteamiento además de permitir la creación de un nuevo paradigma, que antes no estaba contemplado socialmente, está basado en algunas teorías como la del comportamiento, las relaciones humanas, y las nuevas relaciones humanas, dado que, ambas tienen componentes que permiten iniciar el descubrimiento de las acciones o motivos por los cuales llevan al empleado o sujeto externo a cometer dicho delito, además perciben al hombre como parte importante de la organización, a diferencia de las teorías clásicas donde se busca incrementar la productividad sin importar el componente humano. Para ello, es importante conocer los conceptos de phishing y organización.

De acuerdo con De la Torre y Quiroz (2020), las organizaciones deben tener sistemas de control interno, combinado con bases éticas y capacitación a empleados, porque en diversas situaciones, son los mismos colaboradores quienes realizan el fraude. Es probable que las organizaciones no se estén percatando de esto, pero es importante, como dicen Zhang, Wang y Kong (2019) que las organizaciones brinden un trato justo a los colaboradores, generando así menos riesgos a ser víctimas de un fraude. Asimismo, sucede cuando ofrecen estímulos como parte de motivación a los empleados, disminuye la probabilidad de ocurrir un fraude en esta por parte de personal interno a la organización, siendo este factor motivacional, uno de los cuales se menciona más adelante en los factores sociales que conllevan al fraude electrónico.

Considerando que quien diseña una estrategia no necesariamente la lleva a cabo o la aplica, es importante que, desde el área de recursos humanos, columna vertebral de una organización, se generan estrategias y/o planes que conlleven, por ejemplo, desde la prospectiva, a construir los escenarios futuros deseados.

Objetivo de la Investigación

Describir los factores sociales por las cuales el empleado y/o externo a una organización decide realizarle un phishing.

Marco de Referencia Teórico

¿Qué es Phishing?

El phishing hace referencia a una de las modalidades de fraude electrónico o cibercrimen, donde se agrupan delitos ejecutados de forma virtual, con la intención de generar efectos negativos en los medios electrónicos y redes de información. Romeo (2007) define el Cibercrimen (fraude electrónico) como:

> Conjunto de conductas relativas al acceso, apropiación, intercambio y puesta a disposición de información en redes telemáticas, las cuales constituyen su entorno comisivo, perpetradas sin el consentimiento o autorización exigibles o utilizando información de contenido ilícito, pudiendo afectar a bienes jurídicos diversos de naturaleza individual o supraindividual (p. 656).

También puede definirse como “un ataque de ingeniería social para adquirir y utilizar ilegalmente los datos de otra persona en nombre de un sitio web legítimo para beneficio financiero o personal” (Sarikaa y Varghese, 2017, p. 3274). López (2019) plantea el phishing como un instrumento de estafa que utiliza la ingeniería social para manipular indebidamente al usuario, con el propósito de lograr beneficios y recolectar información suministrada por el mismo; es un tipo de fraude ejecutado por un phisher, nombre que adopta la persona que comete el engaño, a través del uso de correos electrónicos con

contenidos aparentemente provenientes de entidades e instituciones reconocidas, llamando la atención del usuario para que este proporcione datos confidenciales que posteriormente serán usados con intenciones fraudulentas. Además, agrega que la palabra phishing se deriva del término fishing en inglés, el cual tiene como significado pescar, por lo tanto, dicha práctica ilegal se enfoca principalmente en atrapar a sus víctimas.

Condori (2013, p.34) lo define como “envío de correos electrónicos que, aparentando provenir de fuentes fiables intentan obtener datos confidenciales del usuario, que posteriormente son utilizados para la realización de algún tipo de fraude”.

Rodríguez (2015) concibe el phishing como:

> Una forma de actuación potencialmente criminal que se concreta en la utilización de técnicas de engaño, y/o en la utilización de código malicioso, con el objeto de obtener información confidencial, especialmente referida a datos de identificación frente a terceros, de una persona natural o jurídica. Las técnicas de engaño se refieren a actos que, valiéndose de engaños de diverso tipo, buscan que el titular legítimo de la información haga entrega de tal información (p. 25)

Teniendo en cuenta las anteriores definiciones, puede afirmarse que el phishing corresponde a una suplantación de identidad generada por personas malintencionadas que acuden a los medios electrónicos haciendo uso de credenciales de autenticación en correos electrónicos y redes sociales, facilitando la obtención de nombres de usuarios y contraseñas; generando consecuencias como pérdidas monetarias no solo a personas naturales sino también a organizaciones.

El fraude electrónico o cibercrimen comprende una cantidad considerable de modalidades que han sido creadas y desarrolladas en base a objetivos y necesidades provenientes de individuos que centran sus intereses en medios magnéticos para sacar provecho de éstos de formas inadecuadas. En la Tabla 1 se describen las modalidades más relevantes.

Tabla 1

Modalidades de Fraude Electrónico

Autor	Modalidad	Concepto
Acurio del Pino (s.f.)	Data Diddling o manipulación de datos de entrada	Alteración desautorizada de datos, buscando generar movimientos indebidos en transacciones que realizan las empresas.
Fuentes, Mazún y Cancino (2017)	Manipulación de programas o troyanos	Su principal objetivo es brindar acceso a quien está a cargo del fraude, otorgándole autoridad para ejecutar administraciones remotas no autorizadas en los servidores intervenidos.
Acosta (2012)	Sabotaje informático	Funciona bajo técnicas como virus informáticos y malware, los cuales facilitan la modificación y borrado de datos en los sistemas informáticos, dificultando su normal desempeño.
Acosta (2012)	Espionaje y hurto informático (data leakage)	Divulgación de datos reservados de forma no autorizada, generalmente de empresas, ocasionando significativas pérdidas económicas.

Monsalve (s.f.)	Ingeniería Social	Práctica utilizada con intenciones persuasivas derivadas de la psicología, aprovechándose de las emociones de las personas y situaciones donde estas pueden reaccionar de forma predecible, y de este modo lograr acceso a sistemas de datos, e indagar en aspectos personales privados, que pueden llegar a ser utilizados en contra de las víctimas.
Goujon (2013)	Phishing	Perpetrado por individuos que se aprovechan de las debilidades de las redes o sistemas informáticos, obteniendo credenciales de acceso de correos electrónicos, redes sociales, sustituyendo entidades para solicitar a las víctimas datos protegidos o privados.

Fuente: Elaboración propia, fundamentado en (Acurio del Pino, s.f; Fuentes, Mazún y Cancino, 2017; Acosta, 2012; Monsalve, s.f; Goujon, 2013).

En cuanto a la organización puede definirse como el conjunto de personas que trabajan para conseguir un fin en común, realizando cooperación o trabajo en equipo, para el logro de los objetivos. También hace referencia a una institución donde se encuentran personas y recursos materiales (equipos de cómputo, maquinaria, entre otros) para conseguir unas metas y fines previamente trazados. Constantemente hacemos parte de diferentes organizaciones: desde el nacimiento cuando pertenecemos a una familia, cuando vamos al colegio, a la iglesia, al trabajo, entre otros.

Origen e Historia del Phishing

El término phishing proviene de la palabra fishing que traduce pescar, así, el fin último de quienes cometen este tipo de delitos es precisamente “pescar” por medios electrónicos la información de personas o empresas, sin previa autorización, generando con ello impacto económico y social.

En cuanto a las iniciales Ph, este se usa dado la transformación a la palabra fishing en phishing que frecuentemente los hackers o personas con amplios conocimientos tecnológicos, que ingresan a sistemas informáticos sin previa autorización se distinguían como phreaks (Leguizamón, 2015), aquellos que tienen mucho conocimiento tecnológico-telefónico, y usan ese conocimiento para obtener información personal no autorizada. Con la relación existente entre hacker y phreaks viene el Ph inicial del phishing, aludiendo a un uso inadecuado de la tecnología.

En relación a la historia, el phishing se usó inicialmente en 1987 durante la conferencia *“sistema de seguridad: la perspectiva de un hacker”,* donde se intentaba argumentar sobre una técnica para la imitación de una organización conocida; aunque el término se utilizó por primera vez en la empresa estadounidense AOL que suministra servicios para acceder a internet, y ese acceso provocó que el phisher distribuyera software falsificado; misma empresa que empezó con los ataques de phishing (Leguizamón, 2015).

Tipos de phishing

El phishing se clasifica de acuerdo con Padilla (2009), según las técnicas sobre las cuales se tiene acceso a la información, como se muestra en la Tabla 2.

Tabla 2

Tipos de Phishing

Tipo de Phishing	Definición
Deceptive Phishing	Se presenta por medio del envío de correo electrónico engañoso, donde se suplanta a una organización de confianza, reconocida, en el cual desde el momento en que la víctima ingresa al enlace que está en el mensaje, es remitido al sitio web falso.
Malware Based Phishing	Consiste en la ejecución de un software de código malicioso en la computadora de la víctima, producto de esta descargar un archivo, ingresar a una página web, abrir un archivo adjunto en un mensaje, ver un video.
DNS Based Phishing (Pharming)	Consiste en modificar el nombre de dominio de una dirección IP sin autorización, remitiendo a la víctima a una IP diferente a la real.
Content-Injection Phishing	En esta clase de ataque, se introduce dentro del sitio web correcto, contenido fraudulento.
Made-in-the-Middle Phishing	La persona que ejecuta el fraude se ubica entre el ordenador y el servidor de la víctima, logrando modificar y filtrar la información a la puede acceder.
Search Engine Phishing	Creación de páginas web indexadas de forma lícita con motores de búsqueda, contienen ofertas llamativas para los usuarios, de forma que este accede e ingresa la información que allí soliciten.

Nota: Elaboración propia, basado en Padilla (2009)

Phishing en las Organizaciones

Una vez definido el phishing, este perpetrado en una organización trae consigo que el defraudador, o la persona que comete el fraude tenga acceso a información de carácter privada de una organización, sin previa autorización de esta, con fines personales (Johnson, s.f.). De acuerdo con CIO México (2020) "*El phishing está haciendo estragos en las empresas de todo el mundo*", y es que constantemente tanto las organizaciones como el ser humano se encuentran altamente expuestas a fraudes electrónicos, que ponen en riesgo su economía. Sin embargo, de las anteriores modalidades de fraude, el phishing es el que mayor representación y repercusión tiene para organizaciones y personas, en la medida en que es el más común, y con la pandemia mundial presentada a raíz del Covid-19, de acuerdo con la encuesta realizada en 2021 por Sophos, se evidencia que el 70% de los encuestados indicaron el incremento presentado en los ataques de phishing desde que inició la emergencia social, donde el sector empresarial mayormente afectado por ello es el gobierno central, con el 77% (Sophos, 2021).

Estructura del Phishing

La herramienta principal por medio de la cual se presenta el funcionamiento de este delito es el correo electrónico y medios digitales. En una organización, por ejemplo, a través del correo electrónico envían información "aparentemente confiable" de un proveedor determinado, con la factura de venta, la empresa abre el correo sin percatarse con el proveedor la procedencia real del mismo, accede al link que dice pagar, diligencia los datos y "paga la factura", sin embargo, ese pago no llegó a la cuenta del proveedor, sino al del estafador o phisher, como se dijo anteriormente. Esta es una de las formas en

que se comete el phishing, ejecución que viene acompañada de estrategia o planificación previa.

Un caso real reportado por el periódico The Boston Globe (2018) consiste en el phishing del cual fue víctima la entidad que fomenta y defiende los derechos de niños, niñas y adolescentes, Save the Children en Estados Unidos, una organización sin ánimos de lucro, en sede Connecticut describen lo sucedido, así:

> Los piratas informáticos irrumpieron en el correo electrónico de un trabajador, se hicieron pasar por un empleado y crearon facturas falsas y otros documentos, para engañar a la organización benéfica y hacer que enviara casi $ 1 millón a una entidad fraudulenta en Japón. Los estafadores afirmaron que el dinero era necesario para comprar paneles solares para centros de salud en Pakistán, donde Save the Children ha trabajado durante más de 30 años. (párr. 2)

Por otra parte, el phishing inicia enviando correos masivos a diversas personas, con información de interés, bien sean promociones, usuarios bloqueados, con mensajes llamativos, al momento de la persona abrir el correo e ingresar a cualquier enlace que se encuentra allí, con apariencia legítima, es direccionado a una página web que no corresponde a la de la entidad en particular, sino que es la del phisher, el cual inmediatamente obtiene la información que requiere para realizar el fraude. De la misma forma ocurre en las organizaciones.

Análisis desde Perspectivas Interpretativas y Prospectiva

Desde la perspectiva interpretativa propuesta por Barba y Montoya (2008) como punto de vista desde el cual se concibe la estrategia, en base a aspectos como la relación dualista entre conocimiento y poder, así como pensar la estrategia organizacional no siempre une procesos racionales sino que proviene de la construcción social; de este modo, el phishing pertenece a este último, basado en la relación existente entre el sujeto que comete el fraude y la organización, aplicando la teoría del actor-red propuesta por Bruno Latour (2008), en la cual se muestra que lo social no se limita solo a personas, sino también interacciones y asociaciones con otros elementos, de la misma manera que, se concibe la figura del actante, a la cual pertenecen los humanos, no-humanos y discursos; también están las asociaciones, donde además de los discursos se encuentra todo aquello que compone la red, como los agentes bióticos y abióticos. Para este caso, las asociaciones entre el sujeto, medio electrónico, y la red compuesta por la organización.

Respecto al punto de vista de la prospectiva, (Astigarraga, 2016, p. 14) la define como “una visión a largo plazo para la toma de decisiones en la actualidad y a la movilización de acciones conjuntas”; en relación a este concepción, es lo que finalmente deben hacer las organizaciones mancomunadamente con el área de recursos humanos, dado que estos son quienes determinan la persona que cumple con requisitos necesarios para pertenecer a esta, y deben por lo tanto considerar esos escenarios futuros con sus colaboradores; implementando incluso planes que conlleven al bienestar laboral, mejorando el ambiente interno, al igual que capacitar constantemente al colaborador en este clase de cibercrimen, dado que, como se ha dicho, puede ser perpetrado por un agente interno

o externo a la organización; esto a pesar que el factor comportamental del ser humano es complejo, como la misma organización. De igual manera, la prospectiva permite la toma de decisiones estratégicas en las organizaciones, por lo cual es importante su uso.

Factores Sociales que conllevan al Accionar del Sujeto o Colaborador a realizar el Fraude Electrónico

Existen múltiples razones por las cuales el colaborador, que se encuentra dentro de la organización puede estar motivado a realizar el fraude electrónico (ver Tabla 3).

Tabla 3

Factores Sociales que conllevan al Fraude Electrónico

Actor	Causa	Motivo
Colaborador / Sujeto	Baja remuneración	Querer aspiración material
Colaborador / Sujeto	Insatisfacción laboral	Factor económico o poca motivación
Colaborador / Sujeto	Cultura	Entorno que roda al individuo (familia, barrio, sociodemográfico)
Colaborador / Sujeto	Estatus	Aspiración material, estrato socioeconómico
Colaborador / Sujeto	Ética	Poca ética profesional y del individuo como tal
Colaborador / Sujeto	Poder	Tener el control para imponer sus decisiones
Organización	Sistema de estímulos	Verificar si tiene, cuáles son
Organización	Recursos humanos	Factores asociados a la selección de personal
Organización	Sistemas de verificación	Validar si tiene sistemas de verificación de chequeos y control de seguridad

Nota. Elaboración propia.

Estos son factores que influyen también en el talento humano, dado que se está mencionando el individuo o persona como tal; dentro de las motivaciones a realizar el fraude, hay una incidencia por ejemplo en el puesto de trabajo del colaborador: puede no ser el más acorde, no estar motivado allí, tener una alta presión sobre los jefes, entre otros. Aunque es importante capacitar los empleados de la organización, de forma que aprendan a diferenciar un correo phishing, y actuar ante el mismo; así como también se hace necesario conocer los motivos que impulsan al individuo cometer un fraude de tal magnitud, para de esta forma, lograr una mejor protección ante eventualidades que ponen en riesgo la economía de las personas y organizaciones.

Descripción de la Metodología

El tipo de investigación es de " enfoque cualitativo utiliza la recolección de datos sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación" (Hernández, Fernández y Baptista, 2007, p. 7). De acuerdo a esto la metodología que se utilizará será de tipo cualitativo, con un diseño documental definida como “una serie de métodos y técnicas de búsqueda, procesamiento y almacenamiento de la información contenida en los documentos, en primera instancia, y la presentación sistemática, coherente y suficientemente argumentada de nueva información en un documento científico, en segunda instancia” (Tancara, 1993, p. 94). Además, no se aplicará a una organización puntual, sino conjuntamente a las organizaciones, de la misma manera que no se utilizarán métodos para recolección de información como encuestas ni entrevistas. Teniendo en cuenta el nivel de investigación, es descriptiva y consiste en “caracterizar un fenómeno o situación concreta indicando sus rasgos más peculiares o diferenciadores” (Morales, 2012, p. 1); esto dado el objetivo de la investigación enfocado en la descripción de un fenómeno.

Conclusiones

1. Es importante realizar investigación acerca del comportamiento, y situaciones, factores que provocan el colaborador de una organización, o sujeto externo a esta se vea motivado a realizar el fraude electrónico phishing, donde una vez se obtiene la confianza necesaria de la organización, puede infectar fácilmente el sistema de la misma, obteniendo información confidencial, sin previa autorización, muchas veces, pensando en un reconocimiento como tal, esto para el caso del colaborador y hasta del sujeto externo a esta.

2. Es una realidad que muchas organizaciones a nivel mundial se han visto afectadas por este tipo de fraude electrónico, sin embargo, a pesar que algunas han fortalecido su sistema de defensa, instalando programas que eviten dicho fraude, lo que puede verse como algo “normal”, el hecho de estudiar estas situaciones en diferentes organizaciones y países, implica el contemplar al ser humano como principal actor de la red llamada organización.

3. El factor motivacional dentro de las organizaciones es considerado entre las principales causas por las cuales el colaborador toma la decisión de realizar actividades delictivas como fraude, yendo incluso en contra de sus principios y ética, muchas veces buscando su bienestar o en venganza a la empresa por algún motivo que le haya disgustado (disminución de salario, falta de reconocimientos, inconvenientes con los superiores, entre otros).

4. Así mismo como una organización invierte en la instalación e implementación de software de última tecnología, equipos modernos, en búsqueda de obtener una

ventaja competitiva frente a otras organizaciones, se debe invertir en programas o plataformas que conlleven a la mitigación del riesgo ante fraude electrónico, así como en el componente humano, principal actor de una organización. Esto con el diseño de estrategias o planes.

5. El phishing tiene una influencia directa en las organizaciones debido a la fragilidad que se presenta a veces por falta de rigurosidad en los diferentes sistemas de control interno y a nivel organizacional afecta directamente el talento humano, el capital y el marketing de las empresas en la cuales se han tenido una afectación de este.

Referencias

Acosta Semblantes, B.E. (2012). Los delitos informáticos y su perjuicio en la sociedad. [Tesis de pregrado, Universidad Técnica de Cotopaxi]. Repositorio digital UTC. http://repositorio.utc.edu.ec/handle/27000/197

Acurio Del Pino, S. (s.f.). Delitos informáticos: generalidades. http://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Astigarraga, E. (2016). Prospectiva estratégica: orígenes, conceptos clave e introducción a su práctica. *Revista centroamericana de administración pública*, (71), 13-32.

Barba Álvarez, A., & Montoya Flores, M. T. (2008). El análisis estratégico: una perspectiva interpretativa. *Convención Científica de Ingeniería y Arquitectura, XIV Convención Científica de Ingeniería y Arquitectura*, 1-7.

CIO México (2020). Phishing afectó a un 90% de las empresas en el mundo en 2019. https://cio.com.mx/phishing-afecto-a-un-90-de-las-empresas-en-el-mundo-en-2019-estudio/

Condori Velásquez, M. E. PHISHING. *Revista de Información, Tecnología y Sociedad*, 34.

De La Torre Lascano, C. M., & Quiroz Peña, J. I. (2020). Fraude organizacional. Percepciones previas a la creación de un observatorio del fraude. *Economía Coyuntural*, *5*(3), 159-195.

Domínguez, A. H. (2018). Sistema para la detección de ataques PHISHING utilizando correo electrónico. *Telemática*, *17*(2), 60-70.

Fuentes, T., Mazún, R. & Cancino, G. (2017). Perspectiva sobre los delitos informáticos: un punto de vista de estudiantes del Tecnológico Superior Progreso. Advances in

Engineering and Innovation. 2(4), 1-8. www.progreso.tecnm.mx/revistaAEI/index.php/aei/article/view/20/30

Gabaldón, L. G., & Pereira, W. (2008). Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico. *Sociologías*, 164-190.

Giraldo, J y Duarte, I. (2018). Ingeniería Social. Técnica de ataque phishing y su impacto en las empresas colombianas. https://repository.unad.edu.co/bitstream/handle/10596/27050/jpgiraldoma.pdf?sequence=1&isAllowed=y

Goujon, A. (2013). ¿El fin de las contraseñas? http://www.eset-la.com/pdf/prensa/informe/doble_autenticacion%20_el_fin_de_las_contrasenas.pdf

Hernández, Fernandez & Babtista. (2007). METODOLOGIA DE LA INVESTIGACION. 4ta Edicion. Mc Graw Hill

Johnson, L (s.f.). Los riesgos del phishing para las organizaciones. https://etic-solutions.net/etic/los-riesgos-del-phishing-para-las-organizaciones

Joyanes, L. (2017). *Industria 4.0: la cuarta revolución industrial*. Alpha Editorial.

Latour, B. (2008). Re-ensamblar 10 social. *Una introducción a la teoría del actor-red. Buenos Aires: Manantial*.

López, J. (2019). Métodos y técnicas de detección temprana de casos de phishing. Universitat Oberta de Catalunya. Recuperado de http://hdl.handle.net/10609/89225

Martínez, M. (2013). La teoría de Herzberg. https://www.eoi.es/blogs/mintecon/2013/05/15/la teoría-de-herzberg/

Monsalve, J. (s.f). Ciberseguridad: principales amenazas en Colombia (ingeniería social, Phishing y DoS). Universidad Piloto de Colombia. Repository.unipiloto.edu.co/bitstream/handle/20.500.12277/4663/00004883.pdf?sequence=1&isAllowed=y

Morales, F. (2012). Conozca 3 tipos de investigación: Descriptiva, Exploratoria y Explicativa. *Recuperado el*, *11*, 2018.

Pacheco, J. J. R. (2022). El Fraude Electrónico desde el Contexto Jurídico Venezolano. *Revista digital La Pasión del Saber*, *12*(22), 11-21.

Padilla Espinosa, M. J. (2009). Pescando Información Phishing.

Rodríguez Puentes, M. (2015). Responsabilidad bancaria frente al phishing. *Facultad de Derecho, Ciencias Políticas y Sociales*.

Ruiz Navarro, D. B. (2021). Fraude en el sector asegurador por medios electrónico.

Sarikaa, S. & Paul, V. (2017). Parallel phishing attack recognition using software agents. Journal of Intelligence & Fuzzy Systems 32(5), 3273-3284. https://tdeabasesdedatosezproxy.com:2128/10.3233/JIFS-169270

Semana (2021). Estos son los tres ciberdelitos de mayor impacto en Colombia en 2021. https:///colombia/mas-regiones/estos-son-los-tres-ciberdelitos-de-mayor-impacto-en-colombia-en-2021/

Solís Santos, C. (2010). Una revolución del siglo XX. En La estructura de las revoluciones científicas (3a, pp. 9–43). Fondo de Cultura Económica.

Sophos. (2021). Phishing insights 2021. https://assets.sophos.com/X24WTUEQ/at/2x7wmj8mf69r86fv3bgwc4tm/sophos-phishing-insights_2021-report.pdf

Tancara, C. (1993). La investigación documental. *Temas sociales*, (17), 91-106.

The Boston Globe. (2018). Hackers fooled Save the Children into sending $1 million to a phony account. Retrieved 2021, from https://www.bostonglobe.com/business/2018/12/12/hackers-fooled-save-children-into-sending-million-phony-account/KPnRi8xIbPGuhGZaFmlhRP/story.html

Urbina, E. C. (2020). Investigación cualitativa. *Applied Sciences in Dentistry*, *1*(3).

Zhang, J., Wang, J., y Kong, D. (2019). Employee treatment and corporate fraud. Economic Modelling, 85, 325-334. https://doi.org/10.1016/j.econmod.2019.10.028