Revista de Climatología
Volumen 23 Edición Especial Ciencias Sociales

Vol. 23 (2023): 1138-1148 ISSN 1578-8768

El Correo electrónico, como medio de intrusión del Phishing y fraude informático

Yolanda Maribel Mercedes Chipana Fernandez[1]*,Miguel Angel Osco Escobedo[1], Ruben Quispe Ichpas[1],

Gaby Jessica Nieto Fernández[1], Gladys Beatríz Garcia Quispe[1], Dante Aliaga Cerna[1]

[1] Escuela de Posgrado. Universidad César Vallejo. Lima. Perú.

*Autor para correspondencia: Yolanda Maribel Mercedes Chipana Fernandez, ychipana@ucv.edu.pe

(Recibido: 20-06-2023. Publicado: 20-07-2023.)

DOI: 10.59427/rcli/2023/v23cs.1138-1148

Resumen

El cibercrimen ha registrado durante los últimos años un alto índice de fraude informático, mediante el empleo del correo electrónico en la modalidad del phishing, generando una alarmante preocupación en los usuarios de esta herramienta tecnológica. El objetivo de la presente investigación fue identificar y examinar la mejor evidencia científica disponible en relación con el electrónico y del phishing como medio de intrusión ilegal, modalidad incidida del fraude informático. Esta revisión teórica con fuentes secundarias se realizó bajo la metodología de analisis sistemático, disponible en la base de datos Scopus, Scielo, Web of Science, Pro Quest, Redalyc, Ebsco y latindex, de forma gratuita y en español de los últimos 5 años. Se utilizó la búsqueda y verificación de producción científica filtrando los términos de: "correo electrónico", "cibecrimen", "phishing", y "fraude informático", descartándose artículos que hayan sido publicados en el 2017 o antes, y que no estén disponibles para su descarga gratuita. De los resultados obtenidos se desprende que el análisis y discusión de cada uno de los artículos, evidenció la importancia de cultivar una conciencia de seguridad en el empleo y manejo de los correos electrónicos, estableciéndose una cultura digital con medidas acertadas para prevenir el ataque de phishing en perjuicio de personas y organizaciones, evitando las consecuencias del fraude informático que en la actualidad es el ciberdelito con mayor incidencia en cibercriminalidad.

Palabras claves: *Correo electrónico; cibercrimen; phishing; fraude informático.*

Abstract

Cybercrime has registered a high rate of computer fraud in recent years, through the use of email in the form of phishing, generating alarming concern among users of this technological tool. The objective of this research was to identify and examine the best scientific evidence available in relation to electronic and phishing as a means of illegal intrusion, a modality of computer fraud. This theoretical review with secondary sources was carried out under the systematic analysis methodology, available in the Scopus, Scielo, Web of Science, Pro Quest, Redalyc, Ebsco and Latindex databases, free of charge and in Spanish for the last 5 years. The search and verification of scientific production was used, filtering the terms of: .^{em}*ail", çybecrime", "phishing", and çomputer fraud", discarding articles that have been published in 2017 or before, and that are not available for free download. From the results obtained, it can be deduced that the analysis and discussion of each one of the articles, evidenced the importance of cultivating an awareness of security in employment and handling of emails, establishing a digital culture with correct measures to prevent phishing attacks. to the detriment of people and organizations, avoiding the consequences of computer fraud, which is currently the cybercrime with the highest incidence in cybercrime.*

Keywords: *Email; cybercrime; phishing; computer fraud.*

1. Introducción

En la actualidad, las Tecnologías de Información y la Comunicación, los servicios y productos digitales dirigen cada vez más las actividades de los seres humanos en el mundo. Además, con el advenimiento de la comunicación por email, los correos electrónicos no solicitados, se han convertido en una grave amenaza a la seguridad global y la economía por su versatilidad y facilidad de comunicación Gangavarapu et al., (2020). El enorme crecimiento de las tecnologías en Internet ha cambiado la interacción del usuario en línea y ha generado preocupaciones en la seguridad muy graves. Los desafíos emergentes del mundo no solo se dirigen al dispositivo del usuario, sino que podría hurtar su identidad y dinero Salloum et al., (2021). Las agresiones de ciberseguridad podrían tener éxito porque las personas no son conscientes de sus inseguridades, por la carencia de conocimiento sobre sus secuelas y riesgos; en vista que los cibernautas de las redes sociales tienden a hacer partícipes de sus vidas en línea. Por consiguiente, resulta más fácil para los ciberdelincuentes hallar formas de seleccionar información sobre sus actividades y emplearlas para convencer de que su identidad y sus propósitos son legítimas Desolda et al., (2021).

Cabe resaltar, que la ascendente popularidad de las redes sociales ha llevado a la migración de ataques de phishing a estas aplicaciones. Por lo tanto, el phishing simboliza una grave amenaza para los usuarios de las redes sociales y los phishers se enfilan a un gran número de víctimas en distintas plataformas como Facebook, Instagram, Twitter y muchos otros Parker et al., (2020). La Ingeniería Social y la técnica del phishing son elementos que evolucionan con el paso de los años, en esencia a través del correo electrónico, herramienta de comunicación más empleada en el mundo. Los correos electrónicos de phishing por lo general están vinculados con la ingeniería social y pueden expresarse mediante enlaces y/o archivos adjuntos en este modelo, los cuales se propagan pirateando información personal íntima o el control total del dispositivo electrónico y vía E-mail sin que las personas se den cuenta Gomes et al., (2020).

Las corporaciones inciden en pérdidas financieras y de imagen significativas porque sus operarios son víctimas de los ataques de phishing vía correo. El Informe de ciberdelitos en Internet formulado por el FBI nos hace conocer que en el 2020, se cometieron más de $ 1.8 mil millones en pérdidas debido a ataques de correos electrónicos comerciales, mayor que otro tipo de ciberdelito Jayatilaka et al., (2021). Por otra parte, el reporte del Anti-Phishing Working Group (APWG) difundido en el tercer trimestre de 2020 explicó que la cantidad total de correos electrónicos de phishing descubiertos por el APWG en el indicado trimestre de 2020 ascendió a la cifra de 128,926 ataques, número superior a los 44,497 apreciados en el segundo trimestre del año en mención, y de las 44.008 del primer trimestre 2020 Salloum et al., (2021). Sophos, líder mundial en ciberseguridad, ha propalado resultados en su informe denominado “Phishing Insights 2021”, que muestra que los ataques de phishing conducidos a organizaciones se incrementaron durante la pandemia, ya que sus empleados realizaron teletrabajo desde sus hogares convirtiéndose en objetivos de los ciberdelincuentes Nigeria (2021).

2. Metodología

El método empleado fue un estudio de revisión sistemática de producción científica relacionada al tema, iniciándose con la búsqueda de información en revistas indexadas a nivel de Latinoamérica, Europa, Asia y África en los diferentes repositorios digitales, durante el período del año 2017 al mes de diciembre del año 2022.

El diseño y el sitio del estudio

Se efectuó por medio de una revisión sistemática de artículos de producción científica, cuyo contenido incluía: nombre del autor o autores, año, título, fuente, DOI y referencias. La recopilacion de datos comenzó en noviembre 2021 y finalizó en el mes de enero 2022.

Criterios de elegibilidad

Tipos de participantes: Se incluyeron estudios sobre el fraude informático en perjuicio de los usuarios de los correos electrónicos, mediante la modalidad del phishing, siendo excluidas aquellas revisiones de literatura de naturaleza teórica o que no sean parte del tema investigado. Tipos de estudios: Teniendo en cuenta el número limitado de estudios sobre la presente materia, el objetivo de esta reseña es analizar los conocimientos existentes sobre el tema e identificar en los artículos de revisión, los diseños de estudio, categorías, variables y dimensiones. Tipos de resultados: Se seleccionaron como resultados primarios los siguientes: casos de estudios, investigaciones empíricas, experiencias y similares.

Búsqueda de estudios

Se efectuó una búsqueda manual utilizando referencias de estudios primarios y secundarios encontrados en la búsqueda electrónica. Las búsquedas se realizaron en la base de datos Scopus, Ebsco, Scielo, Pro Quest y Redalyc, para lo cual se tuvo como criterio la consulta por títulos, resumen y palabras clave "Correo electrónico", "delincuencia cibernética", "estafas", "fraude informático".

Selección de estudios

Así pues, el proceso de selección de búsqueda fue realizado por los investigadores. Los estudios se seleccionaron en dos fases. El primer paso consistió en revisar los títulos y resúmenes de las referencias encontradas con diversas estrategias de búsqueda, seleccionándose los estudios elegibles. El segundo paso consistió en revisar el texto completo de los estudios preseleccionados para confirmar su elegibilidad.

3. Resultados

Las estrategias de búsqueda arrojaron 40 artículos. Durante el proceso de selección no se encontraron referencias duplicadas. Los artículos seleccionados fueron leídos para confirmar la elegibilidad. De la revisión de los textos seleccionados se excluyeron a 25 estudios que no cumplían con los criterios de inclusión. (Ver figura 1).

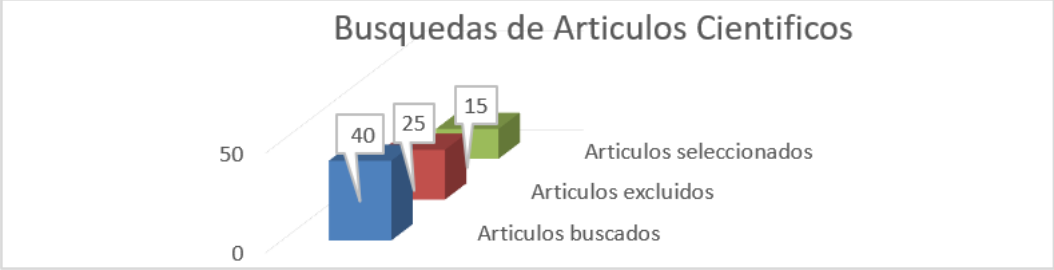

Figura 1: Artículos Científicos utilizados.

Se obtuvo información sobre las bases de datos consultadas, analizando los 15 artículos seleccionados de Scopus 3 artículos lo que equivale al 3,2 %, Ebsco 3 artículos que equivale al 3,2 %, Scielo 3 articulos con 3,2 %, Sage Journals con 1,7 %, Computer Science Computer Networks and Communications con 1,7 %, Gale con 1,7 %, Latindex con 1,7 %, Wos con 1,7 % y ACM Journals con 1,7 %. (Ver figura 2).

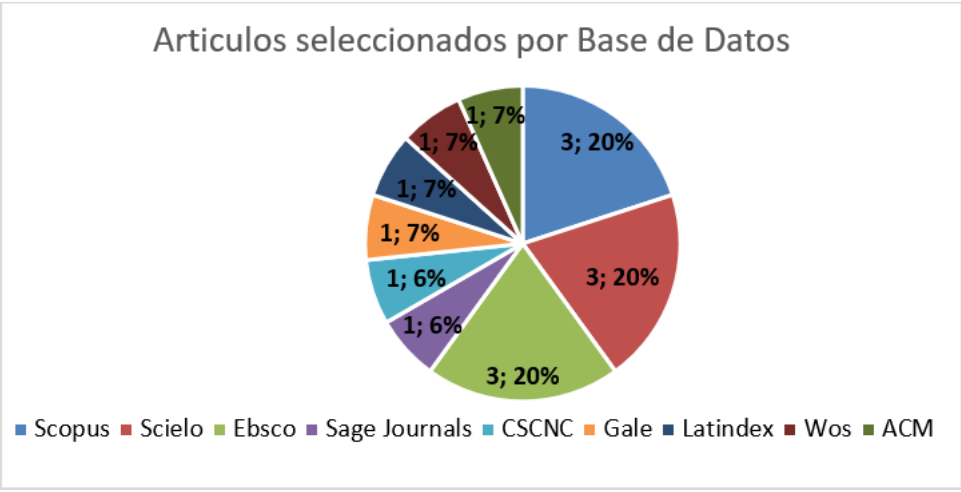

Figura 2: Artículos según base de datos.

Además, se ha graficado los 15 artículos seleccionados por año de publicación, teniendo como resultado que, del año 2021 se tiene 7 artículos que hace un 47 %, del año 2020 se tiene 6 artículos que equivale al 40 % y del 2018 se tiene 2 artículos que equivale un 13 % (ver figura 3).

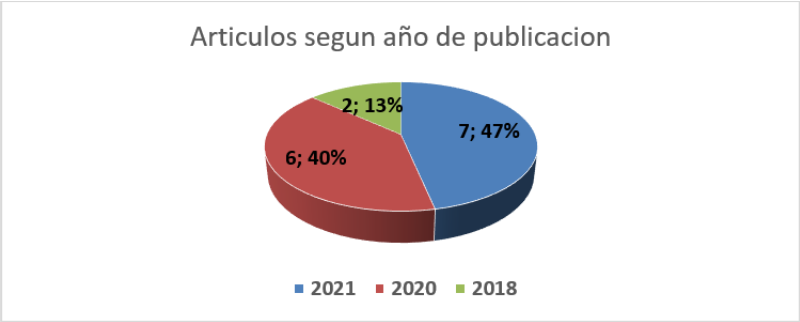

Figura 3: Artículos según años de publicación.

Asimismo, las ubicaciones por países de los 15 artículos, es como sigue, Turquía, Malasia, Sudáfrica, Tailandia, Italia, España, Bélgica, Ecuador y Chile han publicado 1 artículo por cada uno, Colombia 2 artículos y USA 4 artículos (ver figura 4).

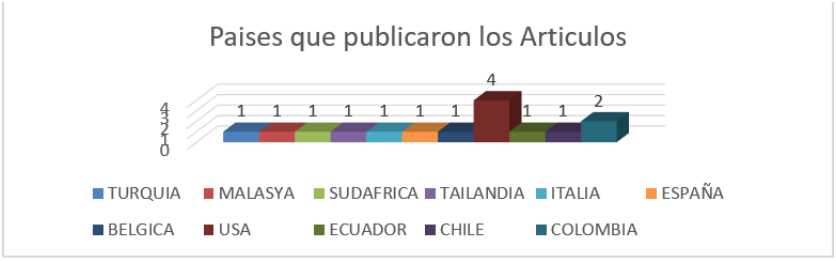

Figura 4: Paises que publicaron articulos.

Los resultados de los 15 artículos restantes se presentan a continuación de forma descriptiva, ya que la naturaleza de estos estudios no permite ningún otro tipo de análisis. En la tabla 1 se presentan los resultados de manera concisa.

Tabla 1: Autores de textos y revistas indexadas que fueron seleccionados por su relevancia.

Autores/ Año/ Título	Base de Datos	Tipo de Estudio	Métodos	Resultados	Conclusiones
Abroshan et al., (2021). El phishing ocurre más allá de la tecnología: los efectos del comportamiento humano y la demografía en cada paso de un proceso de suplantación de identidad.	EBSCO	Artículo de Investigación	Pruebas en línea.	Construcción de un cuadro que prevenga la tentativa del phishing	Contingencias que eleve la posibilidad que el usuario haga clic en un enlace de phishing.
Akdemir et al., (2021). Cómo los phishers aprovechan la pandemia del coronavirus: un análisis de contenido de los correos electrónicos de phishing con temas de COVID-19n.	Diarios sabios	Artículo de Investigación	Método de análisis de contenido cualitativo	Los usuarios admitieron correos electronicos de phishing respecto a las medidas de seguridad de la propagación del coronavirus, tomando la identidad de organizaciones de salud.	Concluyo que las personas se socializaron y laboraron en forma distinta a consecuencia de la pandemia, teniendo en cuenta que la ciberdelincuencia, aumentar alarmantemente el empleo de los correos electronicos de phishing con alusiones al COVID-19.
Alabdan, R. (2020). Encuesta sobre ataques de phishing: tipos, vectores y enfoques técnicos.	Informática Informática Redes y Communicaciones	revistas cientificas	revision de literatura	Se brindó servicios a los usuarios para realizar ataques de phishing mediante estafa informatica	Educar a los usuarios utilizando técnicas para prevenir el phishing
Alex Sumner, Xiaohong Yuan, Mohd Anwar y Maranda McBride (2021) examinando Factores que aumentan la efectividad de las capacitaciones antiphishing, Journal of Computer sistemas de informacion,	Scopus	revistas cientificas	revisión sistemática documental de literatura	Se investigan los efectos de los rasgos demográficos y de personalidad de los usuarios en los programas de capacitación antiphishing y la susceptibilidad del usuario en lo que respeta la identificación de URL de phishing.	aproximadamente el 65% de las organizaciones en los Estados Unidos han sido victimas de un ataque de phishing exitoso.
Almaguer-Perez, D., y Hernández-Yeja, A. (2021). Buenas practicas para el uso seguro del servicio de correo electronico.	Vendaval	revistas cientificas	revisión sistemática documental de literatura	El correo electronico phishing es un tipo especial de mensaje de spam. Dicho correo electronico es un mecanismo penal que se basa en reclamaciones falsas de correo electronico, supuestamente originarias de una compania o banco legítimo.	Actualmente el correo electronico es uno de los servicios más afectados por los problemas de seguridad que proliferan en la Red, tanto en internet como en redes locales o intranet.
Daengsi, T. Pornpongtechavanich, P. y Wuttidittachotti, P. (2021). La seguridad cibernética Mejora de la conciencia: un estudio de los efectos de la edad y el género del tailandés Empleados asociados con ataques de phishing.	Scopus	revistas cientificas	revisión sistemática documental de literatura	Los resultados demostraron que la generacion de edad de los usuarios tailandeses impacta en su conciencia de ciberseguridad.	La ciberseguridad es crucial en la actualidad porque las amenazas cibernéticas (por ejemplo, phishing) se han convertido en una ocurrencia muy comun en la vida cotidiana.
Desolda, G. Ferro, L. Marrella, A. Catarci, T. y Costabile, M. (2021). factores humanos en los ataques de phishing: una revisión sistemática de la literatura.	ebsco	revistas cientificas	revisión sistemática documental de literatura	Un ataque de phishing consiste en enviar un mensaje (p. Ej., Un correo electrónico) que parece ser una organización acreditada (p. Ej., Un banco), suena urgente, afirma incluya informacion importante e invite a las víctimas a abrir un sitio web que es un clon del original	El phishing es el intento fraudulento de obtener información sensible disfrazándose como una entidad de confianza en la comunicación digital.
Eduardo et al., (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura.	Latindex	revistas cientificas	revisión sistemática documental de literatura	Es necesario utilizar gran cantidad de datos para valorar la realidad y rendimiento.	Los ataques más frecuentes de phishing son el spoofing email y el sitio web de suplantación de identidad.
García García, Diego Eloy. (2018). Phishing como delito de estafa informática.	Scielo	revistas cientificas	revisión sistemática documental de literatura	El phishing bancario como tecnica de ingenieria social se caracteriza por intentar obtener información confidencial, comistente en datos personales del usuario, de forma fraudulenta, como pueden ser contraseñas o información sobre tarjetas de crédito u otra información.	El "phishing"se revela como una modalidad de estafa informatica cuyo objeto principal es obtener del usuario, entre otros, datos, claves o números de cuentas bancarias con la finalidad de obtener un beneficio económico ilícito utilizando para ello de forma fraudulenta y mediando engaño datos personales del usuario.
Jayatilaka et al., (2021). Caer en el phishing: una investigación empírica sobre los comportamientos de respuesta de las personas a los correos electrónicos.	ebsco	Informe	Estudio empírico	Las personas hacen clic en enlaces y descargan archivos adjuntos, sin comprobar la legalidad del correo electronico.	El desarrollo de teorías, capacitación y estudios de identidad de correo electrónico de phishing.
Kenneth D. Nguyen, Heather Rosoff, Richard S. (2017). Valoración de la información seguridad de un ataque de phishing, Journal of Cybersecurity.	Scopus	revistas cientificas	revisión sistemática documental de literatura	Los comportamientos de los usuarios son el componente crítico de cualquier sistema de seguridad de la informacion eficaz.	La medida en que los usuarios toman medidas de precaución contra los los riesgos cibernéticos dependen de cómo se perciba el valor de la seguridad de la información en relación con otros objetivos personales importantes.
Mayer Lux, Laura, and Oliver Calderón, Guillermo. (2020). El delito de fraude informatica: concepto y delimitacion.	Scielo	revistas cientificas	revisión sistemática documental de literatura	Se denomina fraude informático a conductas que en verdad corresponde a otros delitos informatica, entre los que destaca el espionaje informático (o hacking) y el sabotaje informático.	Plantear algunas sugerencias para su futura regulación legal expresa, teniendo en cuenta lo que establece el Convenio sobre Ciberdelincuencia del Consejo de Europa.
Ovye John Abari et al., (2020). Tendencias de investigacion de clasificacion de Spam de imágenes de suplantación de identidad: encuestas y problemas abiertos.	Web de la Ciencia	Revision de articulo cientifico	Analisis documental	Imágenes y archivos spam, son empleados por suplantación de identidad.	Los spammers enviaron mensajes utilizandodo imágenes en correos electrónicos de phishing.
Parker, Heather J., y Flowerday, Stephen V. (2020). Factores que contribuyen a mayor susceptibilidad a los ataques de phishing en las redes sociales.	Scielo	revistas cientificas	revisión sistemática documental de literatura	Ante la evolución de las amenazas de phishing, los usuarios a menudo carecen de la conciencia y la capacidad para gestionar estas amenazas.	Ciertas personas son más susceptibles a los ataques de phishing en las redes sociales como resultado de sus hábitos en línea, procesamiento de información, datos demográficos, conocimiento de las (TIC) y rasgos de personalidad.
Rick Wash. (2020) Cómo detectar los expertos los correos electrónicos fraudes de phishing.	Revistas ACM	Artículo de Investigación	Entrevistas personas	Los expertos determinan tres etapas para determinar los mensajes de phishing	Los métodos humanos para localizar el phishing usando información diferente a los métodos técnicos para descubrir phishing.

La primera es una publicación fue realizada por (Abroshan et al., 2021), alude a un artículo de investigación hecho en Bélgica; tuvo como muestra un total de 135 participantes. Debido a que estos fueron de distintos países, se aplicaron pruebas en línea. Se obtuvo como resultado un cuadro total para prevenir con éxito la tentativa de phishing, iniciándose por sus causas principales. Asimismo, se localizó la actitud en la toma de riesgos para predecir el phishing. Se colige que existe un elevado nivel de captación de contingencias que eleva la posible acción del usuario de hacer clic en un enlace de phishing, así también el género femenino es más propenso a dar clic al enlace.

El segundo trabajo presentado por (Akdemir et al., 2021). Refirió a una investigación realizada en Turquía; la muestra consistió en reunir imágenes de correos electrónicos con contenidos sobre el Covid-19. El tiempo de cuarentena tuvo como característica la falta de información y el desconocimiento respecto a esta nueva afección contagiosa. Tanto hombres como mujeres se les conminó a estar en casa, situación que conllevó a gran curiosidad e interés de saber el estado actual de la reproducción del virus. Esta situación fue aprovechada por los ciberdelincuentes, quienes aplicando habilidades de ingeniería social, buscaron aprovechar la voluntad de las personas para obtener información. Se utilizó el método de análisis de contenido cualitativo para rastrear las tácticas de ingeniería social empleados para coaccionar a los usuarios para dar clic en los enlaces que aparecían en los correos electrónicos de phishing. El resultado demostró que a los usuarios a través de sus correos electrónicos se les ofreció, alternativas para prevenir la propagación del coronavirus, a través de mensajes vía correo, tomando la identidad de organizaciones de salud y entidades estatales, obligándoseles a descargar archivos adjuntos facilitados en los correos. Concluyó que debido a la cuarentena se cambiaron la forma en que las personas se socializaron y trabajaron, resultando un mayor riesgo de victimización por la ciberdelincuencia, así como el aumento masivo de dominios sobre el Covid-19 mediante el empleo de los correos electrónicos de phishing con alusiones al COVID-19.

En el tercero, Alabdan (2020), nos precisa en una investigación realizada en Bogotá, Colombia; sobre una revisión exhaustiva de literatura de las propiedades y diferentes técnicas de ataque de phishing. El método empleado fue un análisis de enfoque cualitativo. Respecto a los resultados obtenidos, se precisa que se han proporcionado servicios a los usuarios para ejecutar diversos tipos de ataques de phishing, agraviándolos mediante estafa informática. Se destaca como principal conclusión que el phishing es una dificultad en el mundo, siendo uno de sus vectores principales de propagación, la ingeniería social. La importancia de esta revisión radica en crear conocimiento sobre las diferentes formas de phishing para educar a los usuarios de estos ataques e impulsar el empleo de técnicas para prevenir este ciberdelito.

El cuarto documento expuesto por Sumner et al., (2021) corresponde a una investigación desarrollada en Estados Unidos de Norteamérica. La muestra manejada correspondió a participantes a través de encuestas. El procedimiento utilizado se basó en publicaciones sobre la capacitación en ciberseguridad y susceptibilidad del usuario, desarrollándose preguntas e hipótesis de investigación. Se destacó que el género femenino es más susceptible que el género masculino, asimismo cabe destacar que luego del entrenamiento que se someten las mujeres resultan ser menos susceptibles. Se concluyó que las personas con distintos niveles de educación podrían ser perjudicadas de forma distinta por la capacitación.

En quinto artículo exhibido por Almaguer-Pérez et al., (2021) relató una investigación original realizada en Bogotá, Colombia; se empleó una revisión de los primordiales problemas de seguridad en los servicios de correos electrónicos. El método científico dispuesto por los autores fueron empíricos y teóricos. La importancia de la seguridad del correo electrónico en relación con la información que se envía mediante los mensajes fue el resultado que se obtuvo. Se dedujo que la investigación de la normatividad tanto nacional como internacional en lo que se refiere a la seguridad del servicio vía correo y las advertencias al respecto permitió detallar las acciones a implementar para administrar con eficacia la garantía de un buen servicio de mensajería electrónica.

El sexto artículo enseñado por Daengsi, et al., (2021), atañe a una investigación original realizada en Tailandia. Tuvo como muestra de 20,000 empleados de una institución financiera de Tailandia y se enfocó en la conciencia de seguridad tecnológica. Entre sus resultados obtuvo que de la simulación de phishing, un porcentaje mínimo de empleados abrieron correos electrónicos infectados y otro porcentaje menor no solo abrieron el correo electrónico, sino que además dieron aceptar a los enlaces maliciosos que contenía. Infirió que el conocimiento de ciberseguridad de los trabajadores de Tailandia fue muy aceptable, recomendándose la acción de simular ataques cibernéticos, así como la transmisión de conocimientos, lo cual resulta recomendable para su empleo en otras entidades, siendo el objetivo primordial generar conciencia de ciberseguridad en prevención de ciberataques.

El séptimo título presentado por Desolda et al., (2021) concierne a un artículo de investigación científica hecha en Roma, Italia. Se expuso como muestra la revisión sistemática de literatura. Se utilizó la metodología de Kitchenham, habiéndose obtenido 52 artículos clave de interés publicada entre el 2001 y el 2019. Se demostró que el análisis de las informaciones recuperadas, en relación con los temas de investigación planteadas en la revisión de literatura, contribuye a entender como considerar el factor humano en defensa de los ataques de phishing.

Destaca que para preservar el ciberespacio, los factores humanos representan un papel muy trascendental que los profesionales e investigadores deben tomar en cuenta al diseñar sistemas, algoritmos, organizaciones y todo aquello que implique sistemas informáticos y ciberseguridad.

El octavo artículo entregado por Eduardo et al., (2020) concierne a una investigación original realizada en Ecuador: Se hizo una revisión sistemática de fuente científica documental de literatura para determinar y organizar los distintos tipos de ataque de ingeniería social. Sobre sus resultados se precisó que para encontrar eventos de solución a la cuestión del problema, resultó importante emplear gran cantidad de datos que permitió evaluar la realidad y rendimiento de tal solución. Se coligió que las acciones más frecuentes de ataques de phishing son el spoofing email y el spoofing website y que los medios de atenuación más pertinentes son los algoritmos habituales de Machine Learning a través del Deep Learning.

El noveno artículo expuesto por García et al., (2018) pertenece a una investigación original realizada en Valencia, España. Corresponde al análisis de un pronunciamiento jurisprudencial efectuado por órgano de Justicia de Valencia. Entre sus resultados se colige en la Sentencia de Audiencia Provincial (SAP) de Valencia del 2017, en la cual se condena a una persona como autor del delito de estafa informática mediante la modalidad conocida como "muleros" en la que recepciona parte del dinero transferido por la víctima y entrega otra parte de lo estafado al "phisher", autor del ciberdelito informático. En sus conclusiones, el órgano jurisdiccional de Valencia destaca que el phishing es un ciberdelito informático que viene tomando formas de actuar cada vez más compleja, conllevando al robo de información personal que debe exigir a las agencias bancarias a implementar procedimientos más efectivos para evitar esta sustracción, a través de movimientos bancarios indebidos, evitando que esta estafa cibernética se consuma como delito informático. La importancia y relevancia de este estudio es exigir al usuario tome las medidas de seguridad para protegerse de acceder a enlaces web o cuentas de correo que no pertenezca a la entidad bancaria y no se convierta en víctima de sofisticadas formas de fraude mediante el phishing a través del engaño para acceder a información de sus cuentas bancarias y claves de acceso. Las agencias bancarias desplieguen todas las medidas de seguridad en prevención del fraude informático.

El décimo artículo prologado por Jayatilaka et al., (2021) compete a una investigación original realizada en Texas, Estados Unidos de Norteamérica; tuvo una muestra de 19 estudiantes de la Universidad de Adelaide. El procedimiento que utilizaron fue un estudio empírico respecto al desarrollo de pensamiento de los usuarios al leer sus correos electrónicos. Los resultados que se alcanzaron mostraron que los usuarios hacen clic en enlaces y descargas de archivos adjuntos, sin antes considerar la legitimidad del correo electrónico, ello a consecuencia de sus emociones y rutinas individuales. También hacen clic a correos electrónicos, incluso luego de identificar que son correos electrónicos de phishing o sin estar convencidos de la legitimidad del correo. En sus conclusiones se señalaron que deben desarrollarse teorías de identificación de correo electrónico de phishing, así como elaborar estudios para homologar los hallazgos y así indagar su generalización, también diseñar y evaluar actuaciones más prácticas de educación y capacitación antiphishing. La importancia del estudio determina en detectar con acierto los correos electrónicos de phishing así como disponer de herramientas y técnicas de identificación.

El décimo primer enunciado formulado por Kenneth D Nguyen et al., (2017) relató un artículo de investigación efectuado en los Estados Unidos de Norteamérica. La muestra comprendió un total de 294 adultos americanos. El método dispuesto fue mediante una sesión experimental, seguida de una explicación al detalle, concluyendo con una encuesta. Sobre los resultados se evidenció marcadas diferencias de las personas respecto a la preocupación sobre la seguridad de la información. Se deduce que los comportamientos de las personas son el factor decisivo de seguridad de los sistemas informáticos, también las personas consideran la importancia del cuidado de su información en relación con su exposición en la red.

El décimo segundo artículo ofrecido por Mayer et al., (2020) es una investigación original realizada en Valparaíso, Chile; El método dispuesto fue el de análisis con énfasis en el concepto y delimitación sobre el delito de fraude informático en relación con otros ciberdelitos. Los resultados advirtieron que dentro del concepto de fraude informático se desarrollan conductas de la etapa de delitos tentados o frustrados inclusive a actos de preparación del ciberdelito de fraude, tal como ocurre en la conducta del phishing. Dedujeron la exigencia de regular el delito de fraude informático, tomando como referencia la verificación de la ciberconducta, como la exigencia del cuidado en la manipulación de datos o en plataformas de tratamiento de información. Así como el resultado denominado perjuicio patrimonial ajeno y la asistencia de ánimo de lucro en el ciberdelincuente. El estudio determinó que el fraude informático ha provocado un gran interés por la doctrina penal, ya que constituye una acción indiscutible de la cibercriminalidad, debido a la comisión de fraudes informáticos ligados a transferencias electrónicas de efectivo monetario, convirtiéndose en el centro de delitos informáticos por la consecuencia económica y la frecuente práctica de este ciberdelito.

El décimo tercer entregado por Ovye John Abari et al., (2020) se atribuyó a una investigación original realizada en Malasia; se seleccionaron más de 50 artículos de Web of Science, así como la base de datos de Scopus. El procedimiento utilizado fue de revisión de artículos científicos. Los resultados apuntaron que del análisis de datos de imágenes y archivos spam, son el grupo de datos más empleados en la investigación de imágenes no deseadas en los ataques mediante correos electrónicos de phishing. Finalizaron indicando que los spammers envían mensajes utilizando imágenes con el objetivo de confundir a los usuarios de correos electrónicos de phishing. La importancia del estudio es que nos proporciona un detalle importante de imágenes no deseadas insertadas en correos electrónicos, ya que por lo general los ataques por phishing se basan en textos.

El décimo cuarto artículo presentado por Parker et al., (2020) refirió una publicación académica efectuada en Sudáfrica. La muestra empleada fue material bibliográfico. El método utilizado fue una sistemática revisión de literatura utilizando el paradigma pos positivista, se revisaron un total de 285 artículos mediante cadena de búsqueda empleando bases de datos de revistas indexadas. Respecto a los resultados, estos indicaron que el género femenino entre edades de 18 y 25 años, con pocos conocimientos de seguridad informática y que navegan en redes sociales, están más expuestas a los ataques de phishing. Se destaca que ciertas personas ante los ataques de phishing son más susceptibles en redes sociales como consecuencia de sus hábitos en línea.

El décimo quinto artículo dado por Rick Wash (2020) fue una investigación original realizada en Estados Unidos de Norteamérica; tuvo como muestra a miembros profesionales en tecnología de información de Universidades. El método que utilizaron fue entrevistar a personas con capacidad de identificar mensajes de phishing. Los resultados mostraron que los expertos transitan por tres etapas para determinar los mensajes de phishing, como primera acción se involucran en comprender el correo electrónico empleando su experiencia en el contenido, en segunda acción la sospecha conlleva a que el experto indague el correo electrónico en función a su información que le permita identificar que el correo electrónico es phishing, ante ello se realiza la tercera acción que consiste en ocuparse del correo electrónico. Concluyeron que los métodos humanos para localizar el phishing emplean información diferente a los métodos técnicos para descubrir phishing. La importancia del estudio mencionó que la capacitación actualizada sobre el phishing orientada al análisis de las URL ayuda a reconocer entre un correo que contiene phishing con el que no lo tiene.

4. Discusión

El ciberespacio hoy es parte de nuestras vidas, al igual que el mundo físico, las personas desarrollan sus actividades comerciales, académicas y laborales mediante el empleo de las tecnologías de información y la comunicación, que solo antes realizaban presencialmente. Si bien es cierto el mundo digital en la actualidad ha facilitado las vidas, también es verdad que está generando nuevos desafíos y grandes problemas con el uso de la información. Las diferentes aplicaciones web, así como las redes sociales vienen ganando gran popularidad en los usuarios de la red, siendo este entorno aprovechado por cibrecriminales para ejecutar ataques de phishing en desmedro de la información personal de los usuarios, consumándose en ciberdelitos en sus diferentes modalidades. La pandemia del coronavirus ofreció a los ciberdelincuentes oportunidades para defraudar a las personas aprovechando el interés que se tuvo de protección y cuidado. El presente análisis tiene como objetivo identificar como el phishing puede causar daño a las personas mediante el engaño y la manipulación de la información personal, así como generar una cultura digital en su prevención y desde luego adoptando medidas de seguridad para evitarlo.

A nivel global existió una pandemia sanitaria sin precedentes, sumado a ello el desconcierto por la propagación de información falsa como los “fake news”, sobre el covid, y eso ha sido aprovechado por los phishers, tal como lo refirió Akdemir et al., (2021) en su artículo: Google por medio de inteligencia artificial detectó más de 18 millones de agresiones de phishing y malware en información relacionada con el covid-19 en una semana de abril del 2020, explotando situaciones emocionales y psicológicas, producto del estrés y la ansiedad provocados por la ausencia de socialización como consecuencia de la pandemia.

En su artículo Abroshan et al., (2021) señaló sobre el proceso de ataque mediante correo electrónico de phishing, coincidiendo con el autor al referirse que el phisher remite un correo electrónico a una víctima, el cual puede contener un contacto de phishing o archivo adjunto. El correo podría ser descubierto y paralizado por sistemas informáticos de prevención de este modus operandi antes que ingrese a la bandeja de entrada de la víctima. Al recibirlo podría abrir el mensaje si las técnicas de prevención no le imposibilitan. El segundo paso es cuando la víctima decide hacer clic al enlace que se adjunta al correo o decide abrir el archivo adjunto, esta acción generará que una página web de phishing se abra, y el hacker empleando técnicas de engaño obtenga datos personales, como información de su cuenta bancaria, esto como consecuencia de que el malware solicita a la víctima elija la acción. El tercer paso del procedimiento phishing se ejecuta cuando la víctima envía su información, o decide ejecutar la acción que solicita el malware que implica al dispositivo o cuenta del usuario.

Estos ataques de phishing se propagan mediante la ingeniería social que tiene como propósito manipular a las personas con el fin de beneficiarse, abusando de la confianza, caridad o emociones de la víctima, como lo refiere Alabdan (2020) en su publicación que señala que el phishing emplea como técnica general tres componentes; "La médium" destacándose como medios de interacción de ataque la voz, el servicio de mensajería (SMS) y el Internet. "El vector" canal por donde se realiza el ataque de phishing tales como el correo electrónico, redes sociales, websites, wifi, smishing y vishing y el tercero "Enfoque técnico" que se emplean para obtener acceso a los datos personales de la víctima, tales como el Spear Phishing, el compromiso de correo electrónico empresarial, ataques maliciosos de capcha, Q Rishing y la ya comentada ingenieria social.

Uno de los medios de propagación de este delito son los correos electrónicos que son empleados por los atacantes, quienes se encargan de transmitir los mensajes falsos adjuntos muchas veces a enlaces maliciosos, empleando las llamadas correspondencias spam, definidos como correos no deseados, siendo los spammers quienes emplean técnicas y formas para acceder a las personas, entre ellas a través de mensajes de textos conteniendo imágenes que son insertadas en los correos electrónicos, concordando con lo publicado en su trabajo investigativo por Ovye John Abari et al., (2020) en el cual hizo una descripción de las características empleadas de los atributos de las imágenes en él envió del spam tales como; área de texto, que es el que se inserta en un mensaje; Nivel bajo, que son las características de colores empleadas en las imágenes; Similitud de imagen, que viene hacer la textura expresada en los píxeles de las mismas; Analogía de la región de la imagen, que es la forma y borde que emplea la imagen; Metadatos de imagen, que implican atributos de profundidad, ancho, altura e información detallada del archivo; y por último la ofuscación del texto, que vienen hacer los sonidos o ruidos que puede contener la imagen.

Otro extremo muy importante a considerar es la legitimidad del remitente, los usuarios de correos suelen confiar en la dirección del mensaje para decidir sobre el mismo, toman muy en consideración si esas misivas provienen de personas de su organización o conocidas, sin interesarles lo demás que contenga la comunicación, existe un desconocimiento preocupante, ya que solo o no examinan detalles como nombre de usuario, dominio o subdominio, coincidiendo con Jayatilaka et al., (2021) quien afirmó que la suplantación de identidad se produce cuando los usuarios son engañados por direcciones de dominio falso o remitentes conocidos; son engañados al relacionar nombre de correo y usuarios, así como dominios con la dirección de respuestas o correos phishing del remitente; y también timados si el correo del remitente reviste de confiabilidad en el cuerpo, indicándonos que proviene de ese expedidor; asimismo cuando estos mensajes contienen enlaces los usuarios tienden a tener cuidado con la URL desplazando el cursor encima del enlace y observar en la línea de estado del dispositivo la dirección que muestra y compararla con el dominio de la dirección del correo electrónico remitido, también tienden a analizar que el protocolo de comunicación de la URL del correo tenga el seguro de transferencia hipertexto "HTTPS" que les brinde el indicativo que es seguro.

Los usuarios de correos electrónicos reciben una gran cantidad de mensajes, que presuntamente podríamos decir que se tratarían algunos de ellos de correo electrónico phishing, es ahí donde se genera la incertidumbre del usuario de saber identificar y reconocer cuál es lesivo o no, el autor Rick Wash (2020) en su escrito del cual concordamos, nos muestra que no solo los remedios técnicos son las soluciones para prevenir este delito, sino que los factores socioeconómicos juegan un rol a tomar en cuenta, debido al auge del empleo de diferentes aplicaciones sociales que en la actualidad las personas emplean, por ende es necesario considerar este aspecto, en su estudio realizado con la participación de profesionales de TI, determinaron que para la detección de burglary se aplican tres etapas; el primero el "Sentido", que tiene como objetivo diseñar un ámbito básico del correo que lo ubique en una historia profunda que implique otras situaciones de su vida; el segundo es preguntarse ¿Esto es cyberpunk?, en esta etapa se busca hallar evidencias que les impulse a decidir si el correo es lícito y en la tercera es el "Manejo del medio electrónico", donde muchos de los usuarios toman acciones como borrar estos correos, otros buscan ayuda en organizaciones para protegerse de los ataques y otros tantos tratan de efectuar investigaciones adicionales. En las tecnologías de la información y comunicación se distinguen tres elementos importantes el hardware, el software y el human hardware que se le conoce como el usuario de tecnología, este último elemento en los conceptos de seguridad informática es lo más débil dentro de una organización y es donde los ciberdelincuentes por lo general tratan de vulnerar utilizando ataques de ingeniería social para obtener información personal y emplearlas en perjuicio, siendo uno de los vectores que utilizan para atacar las páginas web y correos electrónicos de scam, la ingeniería social es la acción de lograr obtener de manera fraudulenta información de las personas para utilizarlas en su contra, para el phishing es la forma de adquirir información susceptible a través de los correos.

Asimismo Eduardo et al., (2020) del cual estamos de acuerdo, alude que las formas de ataque de ingeniería social de phishing se realizan en cuatro formas; el "Spoofing email, que se traduce en el envío de correos spam a muchos usuarios a la espera de que alguno caiga en la trampa; el "Fake Social Network Accounts", mediante el empleo de aplicaciones de redes sociales, crea una cuenta con identidad falsa para obtener información de la víctima; el "Hacking", que lo realiza un hacker mediante el empleo de herramientas complejas de software que busca apropiarse de información de la víctima y el "Trojan Hors", que se le conoce como Caballo de Troya, arremetida que se efectúa mediante la ejecución de malware en sistema del dispositivo electrónico de la víctima.

Coincidiendo con lo señalado en su publicación académica por Parker et al., (2020) puntualiza seis dominios de existencia de los correos, que son los sociales, financieros, de seguridad, sanitarios, legales e ideológicos. También indicó que las características que se asocian son las URL dudosas, petición de acción necesaria y errores gramaticales o faltas de ortografía, saludo impersonal y el contenido desacostumbrado fundado en el remitente y el asunto indicados. Así mismo, sostuvo que para reducir la suspicacia del phishing en redes sociales, los usuarios deben conocer fundamentos primordiales de la informática y seguridad, utilizando con frecuencia el internet para incrementar su entendimiento de amenazas online y ataques de ingeniería social, asimismo sugiere que los consumidores deben capacitarse con cursos de formación antiphishing online para conocer cómo detectar estos ataques, además recomienda que los usuarios deben indagar sobre los hábitos en redes sociales.

Ante estos ataques de los ciberdelincuentes que realizan para estafar o suplantar identidad de las personas, es importante hacer conciencia de los daños que pueden producir, es por ello que resulta vital sensibilizar a las personas sobre las medidas que debemos adoptar Sumner et al., (2021) recomienda que hay tres formas importantes de aplacar el phishing el primero la detección del ataque, segundo la educación y por último, capacitación de los usuarios, temas que analizaremos con mayor profundidad en adelante.

Respecto a las medidas que deben de adoptarse para protegerse de las intrusiones informáticas, entre ellas el phishing, es importante precisar que significa la ciberseguridad como acción para hacerle frente Desolda et al., 2021 explicó que estas medidas se traducen en acciones de reducir los riesgos de ataques malignos al software, los dispositivos electrónicos y las redes informáticas, así como el conocimiento de conceptos, políticas, directivas, guías de riesgos de seguridad, buenas prácticas y herramientas tecnológicas para la protección de la organización de TI. De modo que, es muy necesario enfocar estas acciones en la generación de conciencia de seguridad con medidas directas hacia los usuarios o colaboradores que utilizan estos medios, por lo que se coincidió con Daengsi, et al., (2021) en el estudio que ejecutó sobre estos ataques cibernéticos en exámenes de simulacro de ciberseguridad dirigido a empleados de una financiera en Tailandia, determinó que hay factores humanos como el género, la educación, la edad, experiencia en tecnologías y calificaciones universitarias son factores importantes que determinan los comportamientos de las personas en la cultura digital y la adquisición de contenidos en el Internet. Este estudio recomendó el ejercicio de simulación de ataques de correos electrónicos de phishing a los trabajadores de una organización, esto es muy aconsejable, ya que ello permite mejorar y afianzar el nivel de conciencia de ciberseguridad.

La situación de estabilidad de los usuarios de internet respecto a la protección de la seguridad y privacidad de su información personal les preocupa de tal manera que han visto por conveniente recibir beneficios económicos a cambio de proporcionar acceso a datos privados. En su estudio, Kenneth D Nguyen et al., (2017) nos enseñó que algunos usuarios están llanos a sufragar dinero para resguardar su información, apreciándose que la seguridad es para ellos un coste protegido, también descubrió que los usuarios aprecian más los filtros de suplantación de identidad de redes sociales que de los navegadores. De esta forma, respecto a cuan vulnerables se hallan, precisaron que están dispuestos a abonar por un mecanismo de filtración de phishing.

En la actualidad y el confinamiento que viven muchas personas por el problema de la pandemia, ha obligado a desarrollar actividades de teletrabajo desde sus hogares, está siendo aprovechada por los piratas informáticos. Respecto a la criminalidad informática el delito de fraude informático es el ciberdelito con mayor incidencia en el mundo por el impacto económico que representa para las víctimas tanto personas naturales como personas jurídicas que se potencia por el apogeo del comercio electrónico mediante el empleo de correos de comunicación en el ciclo de venta. De esta manera coincidió con Mayer et al., (2020) al delimitar el fraude informático en la siguiente forma: este ilícito suele vincularse con conductas que pertenecen a etapas de ejecución de delito tentado o frustrado, o en algunos casos a actos preparatorios de fraude, este ilícito por lo general, las acciones se desarrollan en operaciones bancarias, también al fraude se le relaciona con comportamientos de otros ciberdelitos, ejemplo se le relaciona al hacking; asimismo también el fraude informático se relaciona con la estafa tal como las legislaciones alemana y española que las regula conjunta o aclarando desigualdades en ambas conductas ya que deslinda el medio que la provoca que en una es el engaño y la otra la manipulación de datos.

Respecto a los bienes jurídicos que lesiona el delito de fraude informático tiene una relevancia patrimonial y un medio comisivo, que es la alteración o manipulación de datos o plataformas informáticas, asimismo tiene este delito un carácter pluriofensivo, ya que su acción lesiona varios bienes jurídicos como la protección de datos y la funcionalidad informática. Respecto a pronunciamientos jurisprudenciales sobre la estafa informática en la forma de phishing, la Sección Segunda de la Audiencia Provincial de Valencia, España, ahonda respecto al phishing, los muleros y la autoría del delito informático, García et al., (2018) en su informe precisó que el 06 de mayo de 2016 que una judicatura dictaminó sentencia (REC. 1402/2016), condenando al autor del hecho delictuoso de estafa informática en tentativa a prisión e inhabilitación del derecho de sufragio. En su doctrina jurisprudencial resaltó al phishing bancario como modalidad de estafa informática, empleando técnicas de robo de datos de cuentas bancarias a través de la suplantación de correos electrónicos phishing o páginas web falsas, siendo el sujeto pasivo los usuarios del servicio online. También analizó la conducta delictiva de los denominados muleros como cómplices del delito de estafa, receptación y blanqueo de capitales.

El Tribunal Supremo estableció que las responsabilidades de este tipo de conductas dan como resultado la comisión del delito de estafa informática que la norma califica y que exige al autor quien despliega el acto de emplear formas de sustracción de datos personales, a través del robo de las contraseñas de acceso a la banca en línea con el fin de obtener un beneficio patrimonial ilegal mediante acciones de engaño en la víctima. Dentro de este escenario, los muleros son colocados para recepcionar los ingresos ilícitos del phishing, correspondiéndole por esta accionar un porcentaje del dinero ilegalmente obtenido, reenviando el resto al autor del ilícito penal.

Respecto a las empresas proveedoras de los servicios de correo electrónico, tienen el gran desafío de brindar sus servicios con garantía, disponibilidad, disminuyendo los peligros de suplantación de identidad, el malware que afectan el funcionamiento del servicio, así como los correos spam. Entonces la seguridad se convierte para el correo electrónico un hecho sensible para analizar con relación a la información. Es importante considerar para ello las diferentes regulaciones, estándares y recomendaciones dentro del ámbito mundial respecto a la seguridad de la información. En consecuencia, hay equivalencia con Almaguer-Pérez et al., (2021) que en su revista científica aludió los primordiales estándares respecto al servicio y seguridad del correo electrónico a nivel global, como: los denominados RFC, Registros federales de Contribuyentes que detalla estándares de seguridad para protocolos de correos electrónicos. RFC 2595, empleado para actualizar conexión con IMAP/POP; RFC 3207, seguridad en el servicio de capa de transporte SMTP, RFC 5246, utilizado para cifrar la conexión; RFC 6376, firmas de dominio de correos para garantizar que no haya sido modificada; RFC 8617, otro, para la cadena de custodia de correos electrónicos; RFC 2045, formatos de admisión de archivos adjuntos y no códigos ASCII; RFC 2047, extensiones de encabezado de mensajes.

5. Conclusiones

De los resultados de la revisión sistemática del presente trabajo del correo electrónico como medio de intrusión del phishing y fraude informático se arribaron a las siguientes conclusiones: Las personas a consecuencia de la pandemia del COVID-19 se vieron obligadas a realizar sus actividades laborales mediante el empleo de las tecnologías de la información y la comunicación en la forma de teletrabajo, situación que viene siendo aprovechada por los ciberdelincuentes, quienes valiéndose de los correos electrónicos de phishing y de los estados emocionales y psicológicos por la ansiedad y la falta de socialización de las personas, efectúan ataques con el fin de obtener sus datos personales. El proceso empleado por el phishing para realizar su ataque, se inicia a través del envío a la víctima de un correo electrónico de phishing adjuntando un enlace o archivo que se ubica en la bandeja de entrada o correos no deseado spam, donde la víctima es seducida a través de textos e imágenes y técnicas de ingeniería social para que acceda y de clic, redirigiéndola a una página web falsa o instalándose un malware en su dispositivo, obteniendo de esta forma acceso a la información personal de la víctima. Las organizaciones y empresas en la actualidad emplean sistemas informáticos utilizando componentes de hardware, software y los usuarios quienes operan esta tecnología, siendo estos últimos el eslabón más débil de seguridad informática, por el cual los ciberdelincuentes vulneran los accesos de seguridad empleando correos electrónicos de phishing mediante ataques de ingeniería social como el Spoofing email, Fake Social Network Accounts y el Trojan Hors. Para hacerle frente a la amenaza de los correos electrónicos de phishing se requiere generar conciencia de ciberseguridad en los usuarios, se deben adoptar medidas para reducir los riesgos de ataque a los dispositivos electrónicos, al software y los sistemas informáticos, debiéndose dictar políticas, directivas, guías para detectar el ataque, así como capacitar a los usuarios, brindarles educación, buenas prácticas, simulaciones de ataques y herramientas tecnológicas de protección, que conlleve a generar cultura digital. En la cibercriminalidad, el delito de fraude informático, en su modalidad de correo electrónico phishing, registra un alto grado de incidencia y perjuicio en el mundo por las consecuencias económicas que genera a las personas y organizaciones públicas o privadas, debido al gran auge del e-comerce en redes sociales y el empleo de la banca online, siendo este ciberdelito un delito pluriofensivo cuya acción lesiona varios bienes jurídicos como la protección de datos y la funcionalidad informática en perjuicio de personas naturales o jurídicas.

6. Referencias bibliográficas

Abroshan, H. Devos, J. Poels, G. y Laermans, E. (2020). Phishing Happens Beyond Technology: The Effects of Human Behaviors and Demographics on Each Step of a Phishing Process, en IEEE Access , vol. 9, págs. 44928-44949.

Akdemir, N., & Yenal, S. (2021). How Phishers Exploit the Coronavirus Pandemic: A Content Analysis of COVID-19 Themed Phishing Emails. SAGE Open.

Alabdan, R. (2020). Phishing attacks survey: Types, vectors, and technical approaches. Future Internet, 12(10), 168.

Alex Sumner, Xiaohong Yuan, Mohd Anwar & Maranda McBride (2021). Examining Factors Impacting the Effectiveness of Anti-Phishing Trainings, Journal of Computer Information Systems.

Almaguer-Perez, D., & Hernández-Yeja, A. (2021). Buenas prácticas para el despliegue seguro del servicio de correo electrónico. Revista Científica, 41(2), 199–212.

Daengsi, T., Pornpongtechavanich, P. & Wuttidittachotti, P. (2021). Cybersecurity Awareness Enhancement: A Study of the Effects of Age and Gender of Thai Employees Associated with Phishing Attacks. Educ Inf Technol.

Desolda, G., Ferro, LS, Marrella, A., Catarci, T. y Costabile, MF (2021). Factores humanos en los ataques de phishing: una revisión sistemática de la literatura. Encuestas de computación de ACM, 8, 1–35.

Eduardo, B., Walter, F., & Sandra, S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: Una revisión sistemática de la literatura. Ciencia y Tecnología, 13(1), 97-104.

Gangavarapu, T., Jaidhar, CD y Chanduka, B. Aplicabilidad del aprendizaje automático en el filtrado de correo electrónico no deseado y phishing: revisión y enfoques. Artif Intel Rev 53 , 5019–5081 (2020).

García García, Diego Eloy. (2018). El Phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (rec. 1402/2016). Iuris Tantum Revista Boliviana de Derecho, (25), 650-661.

Gomes, V., Reis, J. y Alturas, B. (2020). Ingeniería social y los peligros del phishing. Actas del CISTI (Congreso Ibérico de Sistemas y Tecnologías de la Información / Congreso Ibérico de Sistemas y Tecnologías de la Información) , 1-6.

Jayatilaka, A., Arachchilage, NAG y Babar, MA (2021). Caer en el phishing: una investigación empírica sobre los comportamientos de respuesta al correo electrónico de las personas.

Kenneth D Nguyen, Heather Rosoff, Richard S John (2017). Valuing information security from a phishing attack, Journal of Cybersecurity, Volume 3, Issue 3, 7, Pages 159–171.

Mayer Lux, L., & Vera Vega, J. (2020). El delito de espionaje informático: Concepto y delimitación. Revista Chilena de Derecho y Tecnología, 9(2), 221-256.

Nigeria: Report - Increase in Phishing Attacks On Nigerian Organisations Hits 66 %. (2021). allAfrica.com, NA.

Ovye John Abari, Nor Fazlida Mohd Sani, Fatimah Khalid, Mohd Yunus Bin Sharum and Noor Afiza Mohd Ariffin (2020). “Phishing Image Spam Classification Research Trends: Survey and Open Issues” International Journal of Advanced Computer Science and Applications(IJACSA), 11(11).

Parker Heather J. y Flowerday Stephen V. (2020). Factores que contribuyen a una mayor susceptibilidad a los ataques de phishing en las redes sociales. Revista Sudafricana de Gestión de la Información, 22 (1), 1–10.

Rick Wash (2020). How Experts Detect Phishing Scam Emails. Proc. ACM Hum. Comput. Interact. 4, CSCW2, Article 160 (October 2020), 28 pages.

Salloum, S., Gaber, T., Vadera, S., & Shaalan, K. (2021). Phishing Email Detection Using Natural Language Processing Techniques: A Literature Survey. Procedia Computer Science, 189, 19–28.