UNIVERSIDAD ESPÍRITU SANTO

ESCUELA DE POSTGRADO EN DERECHO

EL PHISING COMO CIBERDELITO Y SU CONDUCTA TÍPICA DIFERENCIADA DE OTROS DELITOS INFORMÁTICOS EN EL ECUADOR

TRABAJO DE TITULACIÓN QUE SE PRESENTA COMO REQUISITO PREVIO A OPTAR POR EL TÍTULO DE

MAGISTER EN DERECHO PENAL

AUTORES:

ABG. JOSÉ LIZANDRO CONFORME OJEDA

ABG. NELSON VELA ANDRADE

TUTOR:

DR. SANTIAGO ALEJANDRO ORTEGA GOMERO

SAMBORONDON, DICIEMBRE 2023

El *Phising* como Ciberdelito y su Conducta Típica Diferenciada de otros Delitos Informáticos en el Ecuador

Resumen

Phishing es un término anglosajón que hace referencia a una actitud dolosa dentro de la navegación web, busca el engaño del usuario para poder acceder a sus datos y a sus bienes. En tal sentido, este proyecto tuvo como antecedentes, las referencias sobre el crecimiento de la incidencia de este delito en los ámbitos globales, regionales y locales. Del mismo modo se pudo determinar su objetivo general: analizar los elementos constitutivos del "PHISING" como un nuevo ciberdelito y su conducta típica diferenciada de otros delitos informáticos establecidos en el Código Orgánico Integral Penal. Empleando la metodología de investigación de tipo descriptiva, analítica y documental de campo; con el uso de los métodos inductivo-deductivo y el histórico-jurídico; para lo cual se realizó una recopilación de información a través de un cuestionario que contiene de diez preguntas cerradas. Finalmente se obtuvo como consecuencia a los siguientes resultados: se diferenció que los delitos del COIP, no contenían en sí el tipo de *Phishing*.

Palabras Clave: delito informático, norma penal, tipo penal.

Abstract

Phishing is an Anglo-Saxon term that refers to a malicious attitude within web browsing, seeking to deceive the user in order to access their data and assets. In this sense, this project had as background, the references on the growth of the incidence of this crime in the global, regional and local spheres. In the same way, it was possible to determine its general objective: to analyze the constitutive elements of "PHISING" as a new cybercrime and its typical conduct differentiated from other computer crimes established in the Comprehensive Organic Criminal Code. using the descriptive, analytical and documentary field research methodology; with the use of inductive-deductive and historical-legal methods; for which a collection of information was carried out through a questionnaire containing ten

closed questions. Finally, the following results were obtained as a consequence: it was differentiated that the COIP crimes did not contain the type of *Phishing*.
Keywords: computer crime, penal norm, penal type.

Introducción

El *Phising* a nivel mundial según Asobanca (2022, pág. 1); en el año 2020 se registraron 1.1 millones de compras en línea por minuto; lo que también generaba 4.1 millones de búsquedas en Google y se enviaron 190 millones de correos electrónicos por día. La era de la digitalización ha impulsado que globalmente, la cantidad de ciberdelicuentes aumente de forma exponencial impulsada por la necesidad de hacer actividades en línea por parte de las personas que anteriormente trabajaban en un ámbito físico.

Este problema que afecta desde los ámbitos mundiales, registró desde enero del 2020 hasta enero del 2021 un pico histórico, pues investigadores internacionales ubicaron 245.771 sitios *phishing* o falsos en un solo mes, según el reporte de *Phishing Activity Trend Report* de la organización internacional APWG (2022) que está conformada por 2.200 instituciones de la industria de seguridad, organizaciones no gubernamentales y entidades públicas de los estados.

Por su parte, Gutiérrez del portal Pray Project (2022, pág. 1) indicó que el panorama de las empresas en América Latina indica un aumento del 30% en los ataques cibernéticos, y a su vez, los bancos reportan un aumento del 52% en casos reportados de *Phishing.* Ahora bien, este delito es básicamente dirigido a la banca, tanto a nivel mundial como en la región, a lo que debe incluirse también el aumento del uso de dispositivos móviles para trámites en línea con la banca móvil, lo que se constituye en otro ambiente novedoso en el cual los delincuentes digitales tienen un blanco fácil.

Además, en Ecuador, de acuerdo a lo indicado en el Diario El Comercio por Rosero (2022, pág. 2) la policía nacional reveló que los ciberdelincuentes en el país pueden recibir entre seis mil y nueve mil dólares al mes, sólo con la creación de portales con información no confirmada, en los cuales se puede crear tiendas en línea o simular una banca virtual en la cual se le sustraen los datos a las posibles víctimas. Según las cifras publicadas por el diario,

desde enero hasta septiembre del 2021 se registraron 1.265 investigaciones por delitos informáticos.

Como argumento central de esta investigación se tiene que la normativa vigente de acuerdo al Código Orgánico Integral Penal (2014) no tipifica el delito del *Phishing* de forma específica, sino que más bien, determinar algunas formas de delitos que pudieran aproximarse, lo que dificulta su determinación por parte del agente fiscal y su correspondiente sanción.

Es por esto, que se hace necesario un análisis de los distintos tipos penales existentes en el cuerpo normativo penal y su determinación con respecto al *Phishing* así como, la necesidad de crear un nuevo tipo que pueda cubrir el vacío normativo, pues, la conducta típica debe estar claramente determinada en la redacción de la norma.

Se determinó como objetivo general de esta investigación: Analizar los elementos constitutivos del "PHISING" como un nuevo ciberdelito y su conducta típica diferenciada de otros delitos informáticos establecidos en el Código Orgánico Integral Penal.

A su vez, lo anterior determina como objetivos específicos: (1) Determinar los aspectos doctrinarios y teóricos de los delitos informáticos dentro del Código Orgánico Integral Penal; (2) Evidenciar la necesidad de un cambio normativo y sugerir la creación de un nuevo tipo penal.

Marco Teórico

El Phising

El delito de *Phishing* es un delito informático porque cumple con las características de ser un comportamiento que se aprovecha del uso indebido de tecnologías de la información y de la comunicación para el acceso ilícito de datos informáticos privado y poder usarlos en perjuicio de los sujetos pasivos del delito.

De igual forma es importante indicar que el *Phishing* no se encuentra expresamente tipificado en la norma penal ecuatoriana, a pesar de contar con similitudes normativas con el delito de Interceptación de datos (art. 230) o falsificación informática (art. 234,1). Uno de los análisis que se pudo observar es la existencia de disposiciones generales en cuanto a la

redacción de delitos, sobretodo, el delito de estafa (art. 186), dejando de lado la realidad material de otros delitos, que, aunque parecidos como el *Phising*, hoy no gozan de tipificación legal y propician su impunidad. (COIP, 2014) (Ventura, 2021)

Delitos Informáticos

De acuerdo a Torres (2019, pág. 32), los delitos informáticos, también conocidos como ciberdelitos, son aquellos que utilizan tecnologías de la información y las comunicaciones (TIC) para perpetrarse. Estos delitos pueden ser cometidos de varias maneras, como el acceso no autorizado a sistemas, el robo de información, el fraude en línea, la difamación, el ciberacoso, entre otros.

Para Miró (2022, pág. 213), los delitos informáticos se pueden clasificar en varias categorías, entre ellas:

Delitos de acceso: Son aquellos que se refieren al acceso no autorizado a sistemas informáticos o a la intercepción de comunicaciones. Ejemplos incluyen el hacking, el espionaje, y la denegación de servicio (DoS).

Delitos de contenido: Son aquellos que se refieren a la creación, distribución o posesión de contenido ilegal en línea, como la distribución de material ilegal o la difamación.

Delitos de robo de información: Son aquellos que se refieren al robo de información personal, financiera o comercial. Ejemplos incluyen el *phishing*, el malware y el robo de identidad.

Delitos de sabotaje: Son aquellos que se refieren al daño o destrucción de sistemas informáticos o a la interrupción del servicio. Ejemplos incluyen el ciberacoso, el ciberterrorismo y el sabotaje.

Delitos de comercio electrónico: Son aquellos que se refieren a la comercialización de bienes o servicios ilegales en línea. Ejemplos incluyen el comercio de drogas, la trata de personas y la venta de bienes robados.

Tal como refieren Nazario y Villanueva (2022, pág. 71) *phishing* es una forma cada vez más común de ciberdelito en Ecuador, donde los delincuentes utilizan técnicas de engaño para obtener información personal y financiera de individuos y empresas.

Los delincuentes utilizan principalmente correos electrónicos y sitios web falsos para llevar a cabo el *phishing*. Estos correos y sitios pueden parecer legítimos, pero en realidad están diseñados para robar información personal y financiera de los usuarios. Un ejemplo común de *phishing* en Ecuador es un correo electrónico que parece venir de un banco o una empresa de tarjetas de crédito, y que solicita información personal y financiera.

Otro método común de *phishing* en Ecuador, indicaron Quinde y Cheme (2019, pág. 12) es mediante mensajes instantáneos o redes sociales, donde se solicita información personal o financiera a través de enlaces maliciosos. Es recomendable tener un software de seguridad actualizado en los móviles y computadores personales, así como no compartir información personal o financiera en internet, especialmente en sitios no seguros. El objetivo del delito es robar información personal y financiera de los usuarios para cometer fraude.

En Ecuador, los delitos informáticos están regulados por el Código Orgánico Integral Penal (2014). Según esta norma penal, los delitos informáticos incluyen, pero no se limitan a:

Apropiación fraudulenta por medios electrónicos: Se hace referencia a un fraude informático o con redes electrónicas de telecomunicaciones en el artículo 190 del COIP, para facilitar la apropiación de un bien ajeno de forma no consentida de bienes, valores, derechos, en perjuicio de la víctima quien se considera una tercera persona, lo cual requiere la manipulación, alteración o modificación del funcionamiento de redes electrónicas, programas o terminales, lo que tendría una pena privativa de libertad de uno a tres años.

En este caso, el delito sugiere una aproximación al *phishing*, sin embargo, es específico con respecto al hardware de los sistemas, más no sobre el engaño que impulsa la colaboración de parte de la víctima, quien, en este delito, no consiente la extracción de sus bienes o derechos.

Delitos contra terminales móviles electrónicos: Los artículos 191 al 195, hacen referencia con respecto a la modificación, alteración, irrupción y reemplazo de los datos que contienen los aparatos móviles informáticos, lo que también incluye su comercialización posterior a la alteración de los mismos.

Revelación ilegal de base de datos: El COIP en su artículo 229, hace referencia a la revelación de datos en provecho propio o de un tercero, de datos o información, lo que vulnere el derecho a la intimidad de alguna persona, lo que puede ser sancionado con pena privativa de libertad de uno a tres años.

Interceptación Ilegal de Datos: Según el artículo 230 del COIP, el espionaje o intercepción de datos sin autorización es considerado un delito y puede ser castigado con penas de prisión de tres a cinco años. Esta presenta cinco variantes de conducta típica lo que puede deberse al tipo de irrupción en los sistemas de información y comunicación que pueda hacer el sujeto activo.

Transferencia electrónica de activo patrimonial: Está referida como delito en el artículo 231 del COIP, que indica una conducta con ánimo de lucro de personas que puedan alterar, modificar o irrumpir en los sistemas informáticos para transferir o apropiarse de un activo patrimonial del sujeto pasivo, lo que se sanciona con pena privativa de libertad de tres a cinco años. Esta conducta requiere una conducta de hacking, lo que no involucra el consentimiento de la víctima, esto a diferencia de lo que se considera genéricamente un *phishing.*

Ataque a la integridad de sistemas informáticos: En el artículo 232 de nuevo se hace referencia a la destrucción, daño o deterior de sistemas informáticos lo que puede considerarse un *hacking* en todos los detalles del comportamiento del sujeto activo. En tal sentido, el delito anteriormente descrito sería requisito previo para la ejecución de daño a los programas o sistemas, pues se requiere la introducción sin permiso del sujeto pasivo para luego destruir la información contenida en ellos.

El acceso no consentido a un sistema informático, telemático o de telecomunicaciones: Estrechamente ligada a la conducta de espionaje, lo establece el artículo 234 del COIP, incluye dos formas de comportamiento descritos en los numerales uno y dos, el primero hace referencia a la introducción en sistemas en contra de la voluntad del legítimo usuario de esa información, lo que puede sancionarse con pena privativa de libertad de tres a cinco años; además, en segundo lugar, hace referencia a la modificación de datos del legítimo usuario

quien en ese caso sería la víctima, lo que pudiera ocurrir en cualquier plataforma digital, y estaría sancionado con pena privativa de libertad de tres a cinco años.

Falsificación informática: Este delito fue introducido en la ley Reformatoria al COIP del 30 agosto del 2021, está contenido en el artículo 234.1, y establece dos formas de comportamiento delictivo en sistemas informáticos, como es el engaño en las relaciones jurídicas para introducir, modificar, eliminar o suprimir contenido digital para presentar documentos no genuinos.

Está sancionado con pena privativa de libertad de tres a cinco años, pero, aún no describe del todo el comportamiento del *phishing*. En el numeral dos, se hace referencia al dolo que debe contener este delito, al querer obtener beneficio a través de un documento modificado en un sistema.

Es importante destacar que el COIP establece que las penas se podrán agravar en caso de que el delito se haya cometido a través de medios informáticos o tecnológicos, y también se podrán agravar si el delito afecta a una entidad pública o es perpetrado por servidores públicos en funciones.

Ahora bien, el concepto general del *phishing* involucra un fraude informático de forma inicial, pues requiere del elemento engañoso, además, es un robo de información personal, pues la persona suministra sus datos de manera colaborativa con el delincuente; y finalmente, podría considerarse también una suplantación de identidad, en tal sentido, esta investigación busca desglosar los elementos constitutivos del delito de *phishing* y generar una propuesta para la sanción en casos en los que se debe tomar en cuenta que la conducta se ajusta a diversos tipos de ciberdelito. Al momento de acusar, el funcionario de fiscalía debe considerar a cuál de los delitos tipificados en el COIP, se corresponde de mejor manera la conducta del delincuente de acuerdo al caso en cuestión.

Estado del Arte

En Ecuador, los delitos informáticos apenas se comienzan a reconocer como tales desde el cambio constitucional en 2009 y posteriormente con la nueva codificación penal, en el año 2014, en tal sentido, los estudios al respecto que tratan las mismas variables del

presente paper, son también de reciente data y no abundan como sí podría ocurrir con otros temas en las ciencias jurídicas, para construir este estado del arte, se cree conveniente citar los siguientes estudios similares:

Villón y otros (2018) realizaron una investigación denominada *"Pharming y Phishing: Delitos Informáticos Penalizados por la Legislación Ecuatoriana"*, mismo que tuvo como objetivo analizar los aspectos más importantes del *Pharming* y el *Phishing* como conductas punibles, que pudieran estar incluidas dentro del Código Orgánico Integral Penal del Ecuador, se realizó un análisis de los distintos tipos penales existentes a la fecha y luego de estas definiciones los autores llegan a concluir que no existe una legislación ajustada a la realidad cambiante a nivel tecnológico, que presenta a la normativa penal ecuatoriana evidentemente susceptible a la impunidad.

Por su parte, Mazaquiza (2021) publicó una tesis de investigación más amplia denominada *"El Phishing como delito informático en la legislación ecuatoriana",* que realizó un análisis de la ciberseguridad por medio del uso de tecnologías informáticas y de comunicación, que exploró las opiniones de internautas que fueron víctimas de vulneración de sus sistemas, lo que a su vez irrumpió en sus bienes patrimoniales, su identidad o el uso personal de la información, lo que evidenció una necesidad de generar nuevas políticas públicas que generen mayor seguridad en las conexiones de redes en el país. Este autor, revisa también los tipos penales y refiere como conclusión que en el artículo 186 del Código Orgánico Integral Penal, se hace referencia a la estafa como un acto de engaño en perjuicio patrimonial, sin embargo, esto no describe fielmente la conducta típica del *phishing*, lo que hace complejo sancionar.

Estas investigaciones revisadas, en comparación con la que se presenta, analizan la conducta típica del *phishing* y a su vez las descritas en el Código Orgánico Integral Penal, sin embargo, en esta oportunidad se presenta mucho más amplio con respecto a cada uno de los tipos penales, evidenciando que aún cuando se han hecho cambios en la norma penal, aún no se logra describir exactamente la conducta penalmente relevante del *phishing*, lo que puede impedir su sanción por parte de los juzgadores.

Planteamiento del Problema

Estos fundamentos teóricos conllevan a hacer la pregunta de investigación:

¿Cuáles son los elementos constitutivos del "*PHISHING*" como un nuevo ciberdelito y su conducta típica diferenciada de otros delitos informáticos establecidos en el Código Orgánico Integral Penal?

Análisis

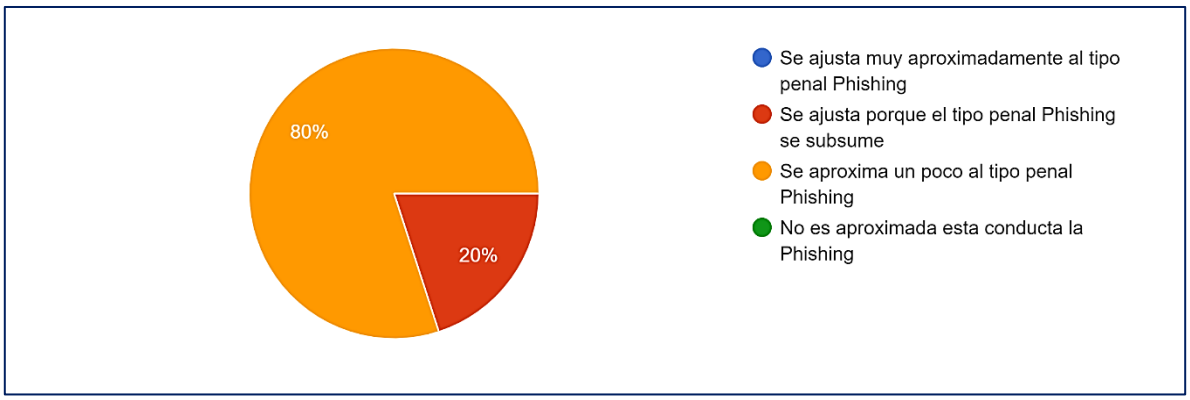
Para obtener insumos necesarios para este análisis, se emplearon técnicas de recolección de datos como la encuesta que a su vez emplea el cuestionario como medio de recopilación, contentivo de preguntas cerradas, dirigidas a sesenta y cinco (65) abogados en libre ejercicio en el ámbito penal ubicados en la ciudad de Guayaquil.

La población sería el total de sujetos de observación, que serían el total de abogados en libre ejercicio en la ciudad de Guayaquil, que, de acuerdo a datos aportados por el Colegio de Abogados del Guayas, se consideran en total unos 35.000 abogados, de los cuales se realizó un muestreo por conveniencia o muestreo no probabilístico, hasta obtener una muestra por disponibilidad de sesenta y cinco (65) abogados. Por tanto, se aplicó la técnica de la encuesta a través de un cuestionario con preguntas cerradas, dirigidas a los abogados en ejercicio en el área penal, los resultados arrojaron lo siguiente:

Figura 1

Pregunta 1. Según el COIP en su Art. 229.

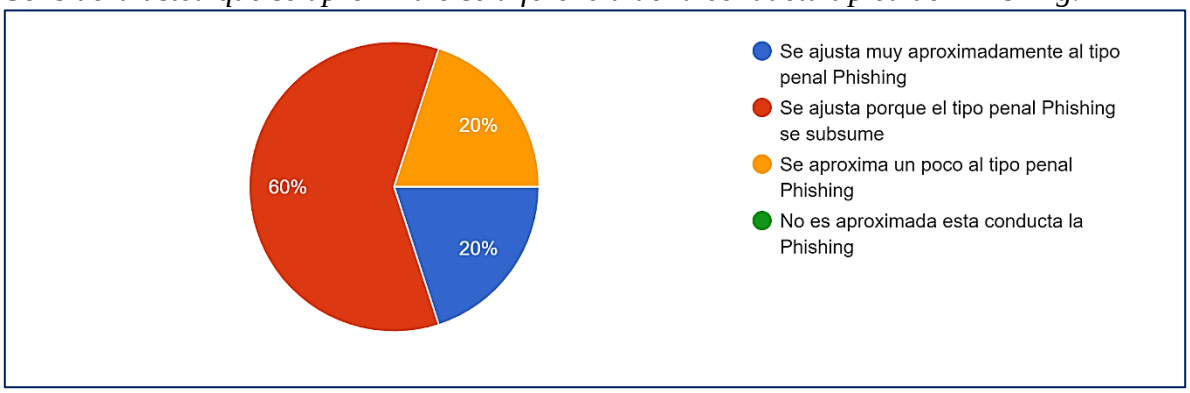
Considera usted que se aproxima o se diferencia de la conducta típica del Phishing



Nota: Elaboración Propia con información del cuestionario aplicado.

Figura 2

Pregunta 2. *Según el COIP en su Art. 230*
Considera usted que se aproxima o se diferencia de la conducta típica del Phishing.

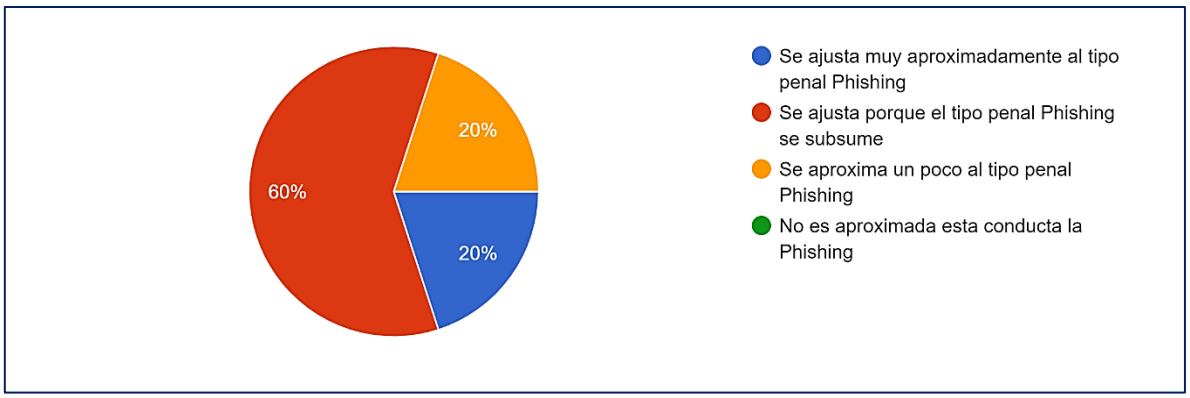


Nota: Elaboración Propia con información del cuestionario aplicado.

Figura 3

Pregunta 3. *Según el COIP en su Art. 231*

Considera usted que se aproxima o se diferencia de la conducta típica del Phishing.

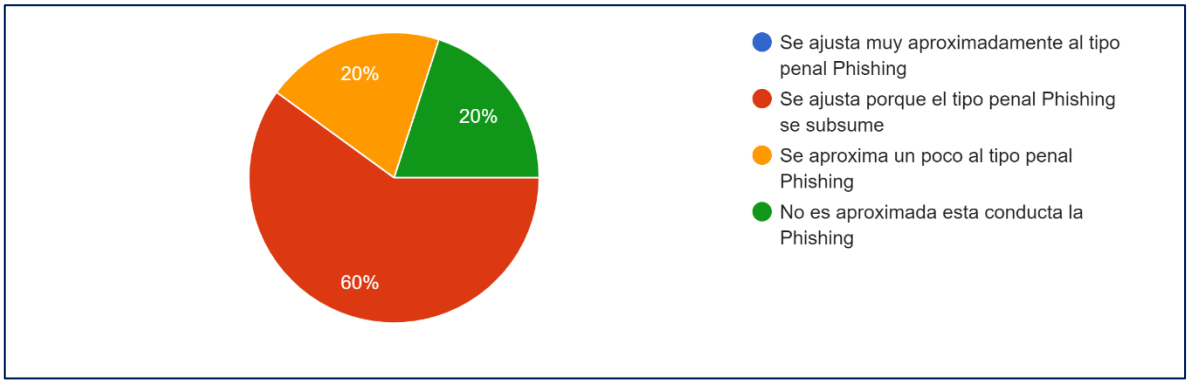


Nota: Elaboración Propia con información del cuestionario aplicado.

Figura 4

Pregunta 4. *Según el COIP en su Art. 232*

Considera usted que se aproxima o se diferencia de la conducta típica del Phishing.



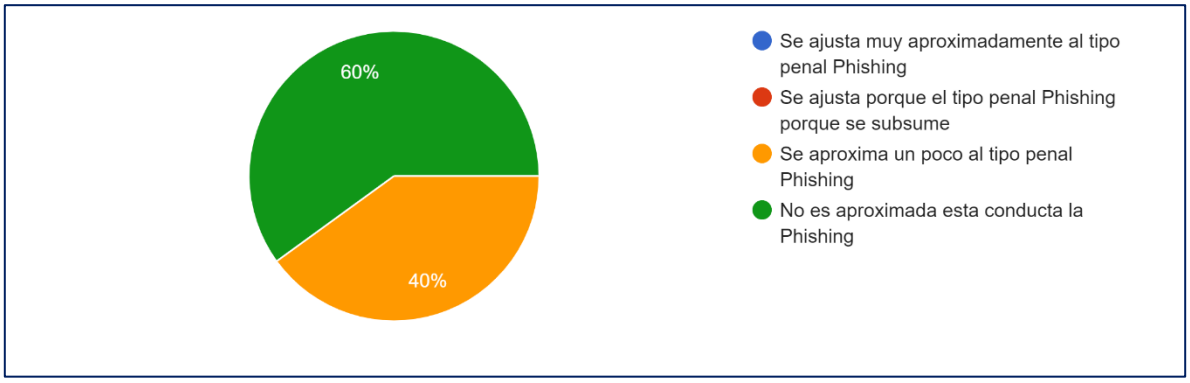
Nota: Elaboración Propia con información del cuestionario aplicado.

Figura 5

Pregunta 5

Según el COIP en su Art. 233

Considera usted que se aproxima o se diferencia de la conducta típica del Phishing.



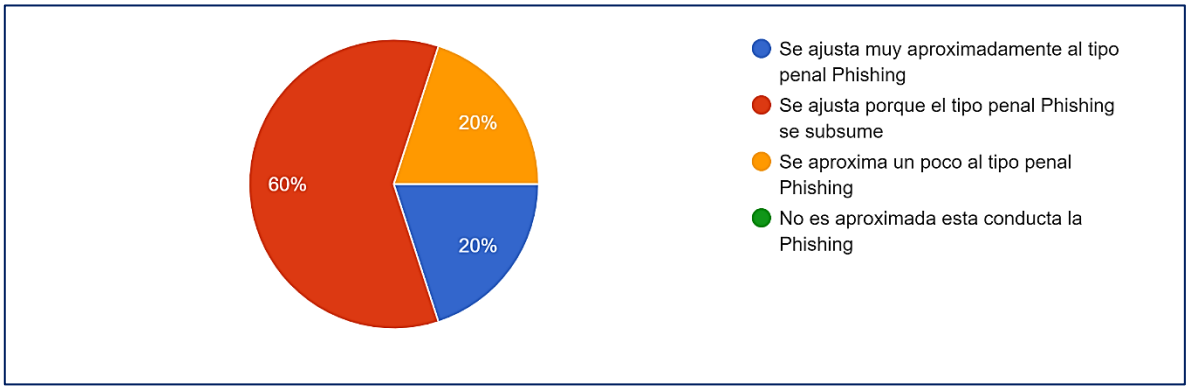
Nota: Elaboración Propia con información del cuestionario aplicado.

Figura 6

Pregunta 6

Según el COIP en su Art. 234

Considera usted que se aproxima o se diferencia de la conducta típica del Phishing.

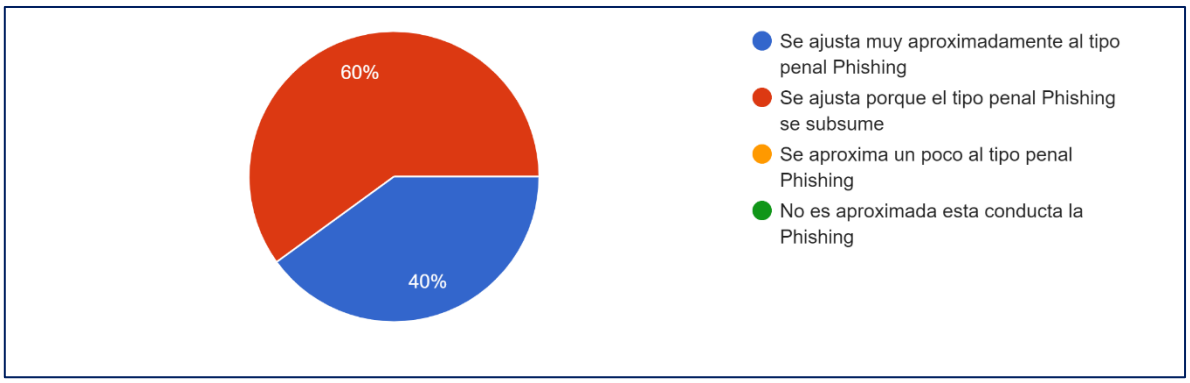


Nota: Elaboración Propia con información del cuestionario aplicado.

Figura 7

Pregunta 7. *Según el COIP en su Art. 234.1*

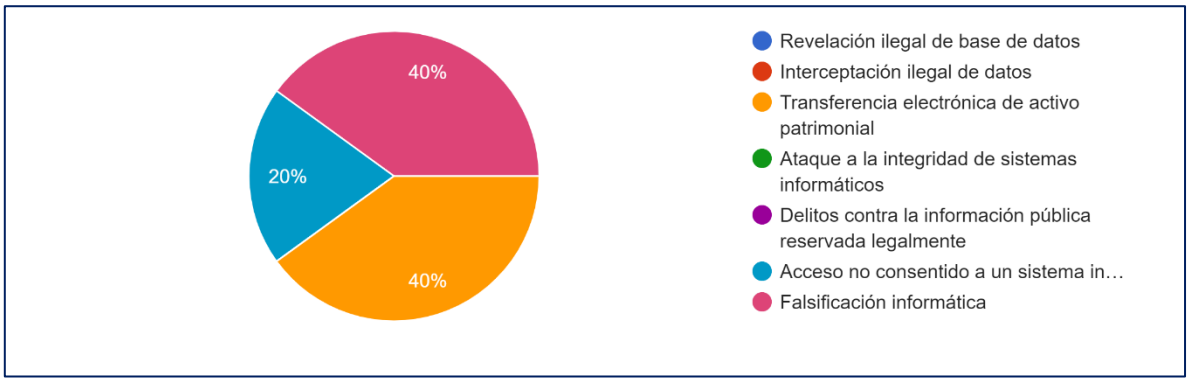
Considera usted que se aproxima o se diferencia de la conducta típica del Phishing.



Nota: Elaboración Propia con información del cuestionario aplicado.

Figura 8

Pregunta 8. ¿De todos los delitos anteriores, cuál considera usted que se aproxima más a la conducta típica del Phishing?

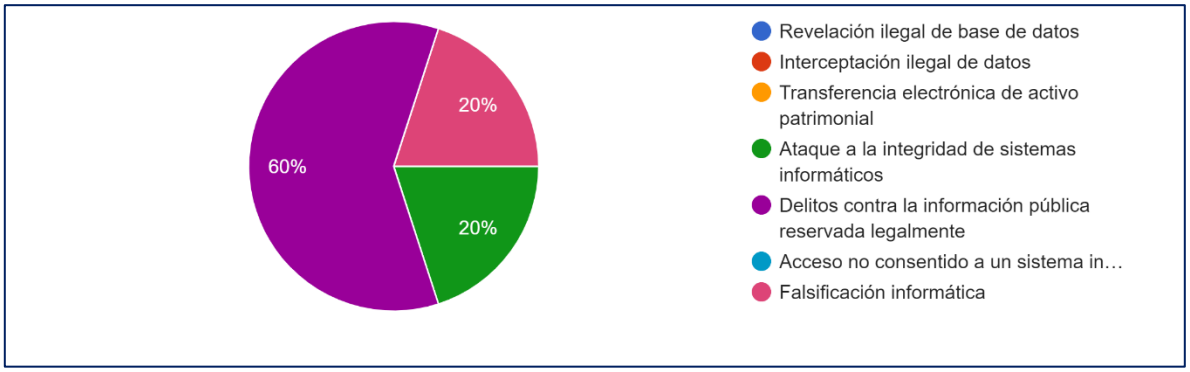


Nota: Elaboración Propia con información del cuestionario aplicado.

Figura 9

Pregunta 9

¿De todos los delitos anteriores, cuál considera usted que se diferencia más a la conducta típica del Phishing?

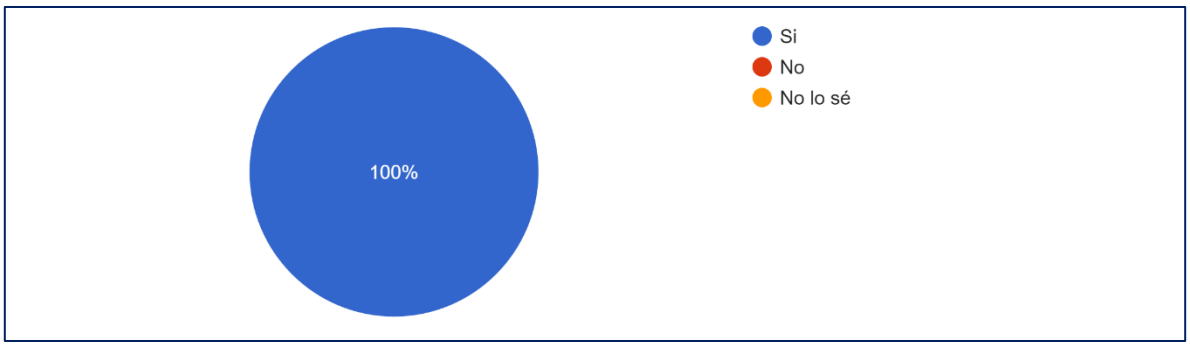


Nota: Elaboración Propia con información del cuestionario aplicado.

En cuanto a la diferenciación del tipo penal normado con respecto al *Phishing*, se tiene que los sujetos consultados indicaron en un 60% que se aleja del concepto de delitos contra la información pública reservada, un 20% a la falsificación informática y un 20% al ataque contra la integridad de sistemas informáticos. De lo que se analiza que el delito de *Phishing* tiene elementos muy distintos del delito contra la información pública reservada, que se constituye en datos dentro de las entidades públicas de la administración del estado. Sin embargo, es importante indicar que la falsificación informática es uno de los delitos que más se aproxima al delito, pese a que los sujetos consultados no lo estiman así.

Figura 10

Pregunta 10. ¿Considera usted que se debe incluir otro tipo penal específico para el Phishing y sus variantes dentro del Código Orgánico Integral Penal?



Nota: Elaboración Propia con información del cuestionario aplicado.

En cuanto a la necesidad de incluir un nuevo del tipo penal que describa específicamente al *Phishing*, se tiene que los sujetos consultados indicaron en un 100% que sí. De lo que se puede analizar que el delito de *Phishing* debe ser incluido como un tipo penal diferente de los descritos en la norma penal actual.

Análisis de los elementos constitutivos del Tipo Penal *Phishing*

Conforme a los aspectos descritos en los resultados de esta investigación se puede indicar el siguiente análisis descriptivo del tipo penal con respecto a los descritos en el Código Orgánico Integral Penal:

Tabla 1

Verbos Rectores	**Apropiarse de forma engañosa**
Tipo de Delito	Delito de resultado
Medio de perpetración	En el medio digital o informático
Bien jurídico protegido	Patrimonio personal, datos personales e información bancaria.
Dolo	Intención de apropiarse de bienes ajenos a través del engaño del usuario digital de sistemas informáticos, tales como: tiendas en línea o banca en línea.
Antijuridicidad	Requiere de la falta de consentimiento, el uso de engaño y la apropiación fraudulenta, también cierto grado de colaboración de la víctima.
Subsunción de otros delitos	Interceptación ilegal de datos, transferencia electrónica de activo patrimonial, falsificación informática.
Pena	La aplicable a un delito compuesto por distintas conductas típicas, lo que generaría un delito grave y una sanción máxima para este tipo de daño causado.

Elaborado por: el autor (2023)

Conclusiones

Luego de realizado el proceso de investigación y al poder cumplir con los objetivos planteados se pudo llegar a las siguientes conclusiones:

1. En Ecuador, el delito informático conocido como *Phishing* no está especificado como tipo penal, por lo que se expuso no sólo en la fundamentación teórica, sino también en las investigaciones comparadas en el estado del arte.
2. Se pudo determinar que los elementos constitutivos del delito de phishing no se encuentran totalmente descritos en ninguno de los delitos informáticos actuales dentro del COIP; tal como se pudo evidenciar en el análisis, no puede coincidir exactamente ninguno de los descritos, más que la estafa, que aún así no logra describir con exactitud los elementos constitutivos del delito de *phishing*.
3. Se evidenció a nivel teórico que el *phishing* se constituye en un delito que consiste en la simulación de un ambiente virtual en el cual se transfieren bienes o patrimonio, con mayor incidencia en la imitación fraudulenta de sistemas bancarios; sin embargo, en Ecuador se evidencia esta conducta en la simulación de tiendas virtuales.
4. Existe una necesidad de reformar la normativa legal vigente para la inclusión del tipo penal *phishing*, ya que ninguno de los delitos actuales lo determina de forma ajustada; lo que pudiera contribuir a una imposibilidad de sancionar esta conducta penalmente relevante.

Referencias Bibliográficas

Acevedo, I. (2017). Aspectos éticos de la investigacióin científica. *Revista Ciencia y Enfermería*, 15-18.

Aredo, L. (2021). *El phishing y su vulneración a la protección de datos personales en los delitos informáticos.* Trujillo, Perú: Universidad César Vallejo.

Arias, F. (2018). *El Proyecto de Investigación.* Caracas: Limusa.

Asamblea Nacional. (2014). *Código Orgánico Integral Penal.* Quito: Registro Oficial.

Asamblea Nacional Constituyente. (2008). *Constitución de la República del Ecuador.* Montecristi: Registro Oficial.

asobanca.org.ec. (julio de 2022). *Los Ataques de Phishing alcazanron su maximo histórico por la pandemia*. Obtenido de https://asobanca.org.ec/innovacion-y-tecnologia/los-ataques-de-phishing-alcanzaron-su-maximo-historico-por-la-pandemia-como-huir-de-ellos/

Castro, J. (2022). *Elaboración de una herramienta de concienciación para dispositivos Android para evitar ser víctima de phishing.* Cantabria, España: Univesidad de Cantabria.

Divito, F. (2021). *Skimming y phishing de tarjetas de crédito o débito: ¿actos preparatorios o principio de ejecución de la defraudación cometida mediante tarjeta falsificada o el uso de sus datos?* Buenos Aires, Argentina: Universidad de San Andrés.

Dos-Nacimento, L. (2021). *Phishing: Aspectos Técnicos y Procesales del Delito estrella en Tiempos de Pandemia.* Madrid, España: Universidad Rey Juan Carlos.

Gutierrez, N. (10 de octubre de 2022). *Estadísticas de Phishing: El panorama en latinoamérica 2022*. Obtenido de Prey Project: https://preyproject.com/es/blog/phishing-en-latinoamerica

Hernández, R., Fernández, C., & Baptista, P. (2018). *Metodología de la Investigación.* México: Mac Graw Hill Interamericana.

Mazaquiza, L. (2021). *El Phishing como delito informático en la legislación ecuatoriana.* Ambato, Ecuador: Universidad Regional Autónoma de Los Andes.

Miró, F. (2022). *El Cybercrimen: Fenomenología y criminología de la delincuencia en el cyberespacio.* Madrid, España: Marcial Pons.

Nazario, N., & Villanueva, L. (2022). *Fraude Informático en la modalidad PHISING y la Necesaria actualización de la legislación para una eficiente y eficaz persecusión penal.* Pimentel, Perú: Universidad Señor de Sipan.

Paredes, E., & Silva, E. (2020). *Responsabilidad civil de los bancos frente al delito de fraude*

informático phising en tiempos de pandemia de Covid 19. Lima, Perú: Universidad César Vallejo.

Quinde, J., & Cheme, G. (2019). *Ciberdelincuencia y el entorno Jurídico Vigente en el Código Orgánico Integral Penal, Autosuficiente, o Hacia una expansión de la Misma.* Guayaquil, Ecuador: Universidad de Guayaquil.

Reyes, M., & Abad, J. (2022). *Transacciones fraudulentas y Delitos informáticos.* Trujillo, Perú: Universidad Privada de Trujillo.

Rosero, A. (11 de Enero de 2022). *El Comercio*. Obtenido de Ciberdelincuentes operan de cuatro formas en el Ecuador: https://www.elcomercio.com/actualidad/seguridad/ciberdelincuencia-ecuador-organizaciones-delictivas-victimas.html

Torres, F. (2019). *La tipificación de los delitos informáticos y su contextualización con el sistema digital y tecnológico.* Bucaramanga, Colombia: Universidad de Santander.

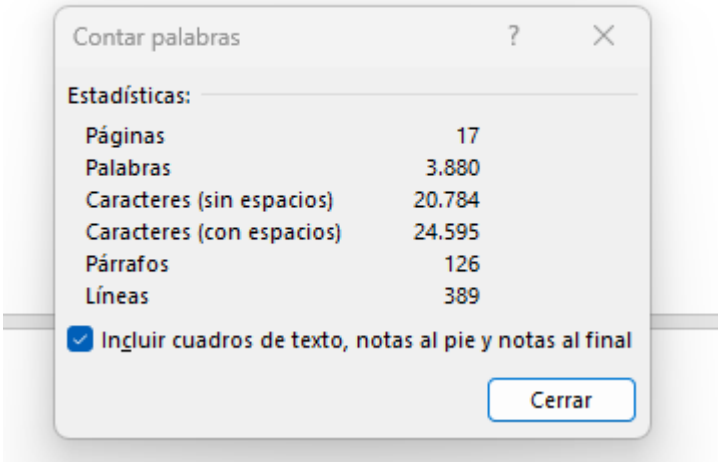
Ventura, M. (2021). *La Tipificación del Phishing, Smishing y Vishing en Nuestro Sistema Penal Peruano, para la Lucha Contra La Ciberdelincuencia en Lima.* Lima, Perú: Universidad Privada del Norte.

Vigo, L., & Zavala, K. (2021). *Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras.* Lima, Perú: Universidad César Vallejo.

Villón, H., Sojos, M., Mendoza, C., Guarda, T., & Clery, A. (2018). Pharming y Phishing: Delitos informáticos penalizados por la legislación ecuatoriana. *Revista Ibérica de Sistemas y Tecnologías*, 671-677.

Villón, H., Sojos, M., Mendoza, C., Guarda, T., & Clery, A. (2018). Pharming y Phishing: Delitos Informáticos penalizados por la legislación ecuatoriana. *Revista Ibérica de Sistemas e Tecnologias de Informação*, 671-677.

Vizueta, J. (2011). *Delitos informáticos en el Ecuador.* Guayaquil, Ecuador: Editorial Edino.


Contar palabras
Estadísticas:
Páginas 17
Palabras 3.880
Caracteres (sin espacios) 20.784
Caracteres (con espacios) 24.595
Párrafos 126
Líneas 389
Incluir cuadros de texto, notas al pie y notas al final
Cerrar