UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES.

ESCUELA PROFESIONAL DE DERECHO.

Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú.

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogada.

AUTORA:

Bach. Mengoa Valdivia, Mariel Melissa. (0000-0002-1514-9567)

ASESOR:

Mag. Vargas Huamán, Esaú (0000-0002-95919663)

LÍNEA DE INVESTIGACIÓN:

Derecho penal, procesal penal, sistema de penas, causas y formas del fenómeno criminal.

Lima – Perú.

2021

Dedicatoria:

El presente trabajo se lo dedico a mi amado y adorado hijo, Gustavo Chahuaylla tú que me das la fortaleza para seguir adelante, te amo corazón, de igual manera a mi querido esposo Jimmy Chahuaylla, porque juntos concreticemos nuestros proyectos futuros personales y familiares, también se lo dedico a mi amada hermanita Tracy Mengoa porque sin tu apoyo ni guía no hubiese podido concluir mi tesis, y para mi querido hermano Pedro Mengoa, porque sé que siempre me estarás guiando desde el cielo.

Agradecimiento:

Primero que nada, quiero agradecer a Dios, por acompañarme en cada momento de mi vida, a mis queridos padres, Teófilo Mengoa y Catalina Valdivia por vuestra fortaleza y su confianza puesta en mí y el saber que siempre poder contar con su apoyo y su guía en mi vida, agradecer también a mi adorada hermanita Tracy Mengoa por estar a mi lado y ser mi soporte y sustento en todo momento y de igual manera agradecer a mi asesor Mag. Esaú Vargas Huamán por sus palabras de aliento en cada momento.

Índice de contenidos

ÍNDICE DE TABLAS

RESUMEN

El siguiente trabajo de investigación tuvo como objetivo general determinar cómo el comportamiento del phisher-mule incurre en los delitos informáticos a la luz del Derecho Penal Peruano, por ello, se planteó como supuesto jurídico que el phisher-mule no es una figura claramente establecida y delimitada en la consagración legal de los delitos informáticos a pesar que atentan contra el patrimonio de los particulares.

Además, la investigación presenta un enfoque cualitativo, tipo básico, diseño de teoría fundamentada y nivel descriptivo: El escenario de estudio constó con la participación de abogados del departamento del Cusco, en cuanto a los participantes, se tuvo 10 abogados litigantes.

En cuanto a la técnica de recolección de datos, se usó la entrevista y el análisis de fuente documental teniendo como instrumento la guía de entrevista y de análisis de fuente documental; el método de análisis de información se basó en uno sistemático, hermenéutico, analítico, comparativo, inductivo y sintético.

Se concluyó que la conducta del phisher-mule no se encuentra individualizada para su tipificación en el código penal peruano, por lo que se necesitaría realizar un estudio más profundo para su correcta tipificación e introducción en el código penal o le ley especial.

Palabras clave: punibilidad, phisher-mule, dolo, ignorancia deliberada.

ABSTRACT.

The following work of investigation had as general objective to determine how the behavior of the phisher-mule incurs in computer crimes in the light of Peruvian Criminal Law, for that reason, it was raised as a legal assumption that the phisher-mule is not a clearly established and delimited figure in the legal consecration of computer crimes despite the fact that they attack the property of individuals.

In addition, the investigation presents a qualitative approach, basic type, design of founded theory and descriptive level: The study scenario consisted of the participation of lawyers from the department of Cusco, as for the participants, there were 10 trial lawyers.

As for the data collection technique, the interview and analysis of documentary sources were used, using the interview and analysis of documentary sources guide as an instrument; the information analysis method was based on a systematic, hermeneutic, analytical, comparative, inductive and synthetic one.

It was concluded that the behavior of the phisher-mule is not individualized for its classification in the Peruvian penal code, so a more in-depth study would need to be carried out for its correct classification and introduction in the penal code or the special law.

Keywords: punishability, phisher-mule, fraud, deliberate ignorance.

I. INTRODUCCIÓN

En la actualidad el término phishing (pesca, en inglés) se ha tratado con mayor frecuencia a raíz de los avances tecnológicos, la modalidad de trabajo remoto, el desarrollo del comercio electrónico (e-commerce) y de la banca electrónica, entre otros. El concepto está vinculado con los datos personales que quedan expuestos en el ciberespacio, y que, según Cocchini (2020), grupos criminales especialista en informática, aprovechan para obtener información confidencial de las víctimas; tales como cuentas de correo electrónico, contraseñas, códigos bancarios, acceso a base de datos empresariales (Thangavel, Yaamine, & Nandhini, 2021) lo cual puede derivar en fraude. Propiamente, la actividad consiste en enviar e-mails falsos de forma masiva a los usuarios, aparentando ser de entes públicos o privados de frecuente uso.

Al obtener los datos necesarios, se realizan operaciones fraudulentas de traspaso patrimonial de forma inmediata, a cuentas bancarias en el extranjero a nombre de personas que integran la banda delictiva. Estos fondos son retirados a entidades de pago de otros miembros, en Europa y países bálticos (Quinkert, Degeling, Blythe, & Holz, 2020). En la última fase de la operación, la organización delictiva debe contar con miembros residentes en los países de las víctimas, dispuestos a dispensar los fondos y enviarlos como remesas a los responsables de la organización delictiva (Palominos,2020).

Considerando lo anterior, es necesario destacar que cuando estas organizaciones no tienen miembros en los países de las víctimas, surge la figura del phisher-mule; La palabra mula no es nueva, sino que proviene del término anglosajón “money mule” que significa que una persona realiza transferencias de dinero el cual se obtuvo de forma ilegal en un mismo país a otro donde suele vivir el estafador (Leguizamón,2016). Por lo que, son terceras personas involucradas en el delito que son retribuidas con una comisión económica por cada operación realizada. Previamente, los muleros han realizado apertura de cuentas bancarias para la realización del fraude, retiran prontamente los importes transferidos, después de sustraer su comisión, las consignan por correo postal, entidades de pago o transferencia a personas desconocidas. Este tipo de delitos ha aumentado considerablemente en los últimos años, razón por la cual se realizan estudios para

consolidar su tipificación penal, además de la recaudación de pruebas que permitan identificar responsabilidades penales de los terceros involucrados (mule) en los fraudes.

En el Perú, como veremos más adelante, se ha realizado una importante labor legislativa para lograr la adecuada descripción técnico-legal de los delitos que se agrupan bajo el término genérico de phishing, para así darles tratamiento adecuado en el marco de la prevención y del procesamiento penal de los responsables, así como el resarcimiento de las víctimas. Estos esfuerzos por adecuar y actualizar las leyes a las novedosas modalidades de los delitos de naturaleza informática, corresponde a la preocupación creciente de la comunidad internacional para hallar fórmulas efectivas de prevención frente a hechos ilícitos que por su naturaleza sobrepasan las tradicionales concepciones que se tenían del delito y de las competencias jurisdiccionales para juzgarlo y castigarlo.

El universo de los delitos informáticos o asociados con medios informáticos es muy amplio porque están favorecidos por la práctica ubicuidad de medios digitales de traslado de información a través del uso de redes informáticas que, como internet, trascienden fronteras y desde las cuáles es fácil operar bajo anonimato. Aquí es muy importante destacar que el anonimato, obrar a la sombra o con el uso de una identidad falsa, es una condición específica que caracteriza a este tipo de conductas ilícitas, lo cual favorece su efecto dañoso en la misma medida que dificulta el trabajo de los órganos policiales de investigación.

En el caso específico de este estudio, además de las características generales observadas en los delitos informáticos, resalta el manejo de la información de la víctima, siempre con la intención de lograr acceso a cuentas bancarias o a instrumentos electrónicos de pago o de crédito con los cuales sustraer o aprovechar ilícitamente cantidades de dinero de los titulares.

En este contexto, surge la interrogante que origina la presente investigación ¿Cómo el comportamiento del phisher-mule incurre en delito informático a la luz del Derecho Penal Peruano? De esta se derivan las preguntas específicas: i) ¿Cuáles son los criterios legales existentes para la imputación penal del phisher-mule en los delitos de fraude informático en el Perú? y ii) ¿Cuáles son las implicaciones del

comportamiento del phisher-mule en problemas relativos al dolo y la aplicación de la teoría de la ignorancia deliberada?

Ya en la perspectiva de la **justificación teórica**, la investigación se fundamenta en el análisis de los dispositivos de la Ley Nº 30096 sobre Delitos Informáticos (artículo 8, en concordancia con los artículos 10, 11 y 12) en especial vinculación con el Código Penal (artículo 196 y artículo 196-A numeral 5) y en el Convenio de Budapest sobre Ciberdelincuencia, vigente en Perú desde el 1° de diciembre de 2019. **Metodológicamente** se justifica por abarcar todo el proceso para obtener los datos legales, jurisprudenciales y doctrinales, que permitan la comprensión y generación de respuestas para la problemática planteada. Desde el punto de vista **práctico**, la investigación está orientada a demostrar la confirmación o rechazo de los supuestos jurídicos de los que hemos partido.

En este orden de ideas, el **objetivo general** de la investigación es determinar cómo el comportamiento del phisher-mule incurre en los delitos informáticos a la luz del Derecho Penal Peruano; por su parte, los **objetivos específicos** planteados: son i) Analizar los criterios legales existentes para la imputación penal del phisher-mule en los delitos informáticos en Perú; ii) Analizar las implicaciones del comportamiento del phisher-mule en problemas relativos al dolo y la aplicación de la teoría de la ignorancia deliberada.

Del mismo modo, la investigación se plantea, como **supuesto jurídico general**, que el phisher-mule no es una figura claramente establecida y delimitada en la consagración legal de los delitos informáticos a pesar que atentan contra el patrimonio de los particulares, lo cual pudiera corresponder a la errada o deficiente tipificación de la norma penal para esta clase de delitos. Como **supuesto jurídico específico 1:** las condiciones de punibilidad en el derecho peruano son ambiguas, por existir distintas modalidades de fraudes informáticos y por el origen de los ataques virtuales, puesto que no necesariamente son cometidos por personas presentes en el país de la víctima. El **supuesto jurídico específico 2:** en la normativa peruana la sanción referida a la conducta del phisher-mule no está tipificada como tal, solo alude a ellos como participantes de delitos informáticos, en consecuencia, puede resultar una tipificación insuficiente para un delito que implica amplias consecuencias dañosas.

II. MARCO TEÓRICO

De la revisión literaria, se pueden resaltar los antecedentes internacionales que siguen:

Calderón (2021) en su artículo sobre la punibilidad del comportamiento del mulero o *phisher-mule* en derecho penal español, aporta una sugerencia de solución a un problema que se plantea no pocas veces en la jurisprudencia: decidir bajo qué tipo penal es punible la conducta del mulero o *phisher-mule*. La solución puede aportarse a partir de la valoración de la estadística demostrada de la sentencia del Tribunal Supremo 834/2012 del 25 de octubre del 2012. La tesis está posicionada afirmando que, la conducta del mulero o *phisher-mule* es punible como receptación y no como blanqueo de capitales imprudente o intencional. Entre las conclusiones emitidas, están las siguientes: a) el delito anterior, la estafa informática, se consideran delitos contra el patrimonio (pertenencias); b) el mulero no es ni autor ni cómplice del delito anterior; y, c) de manera esencial, porque la pena de este tipo de delito es más proporcionada que la del blanqueo de capitales, al menor grado de comportamiento del mulero en comparación con el autor de la estafa, su aplicación ha de ser deseada.

Asimismo, Souto (2017) en su investigación sobre las reformas penales de 2015 sobre el blanqueo de dinero trata de observar las tres principales reformas del blanqueo de capitales seguidas por el legislador penal en 2015. El reglamento orgánico 1/2015 de 30 de marzo, a pesar de que dice eliminar los pequeños delitos leves, transforma la mayoría de ellas en delito leve, por lo que amplía los registros anteriores de blanqueo de capitales generando una excesiva manipulación monetaria y social. La Ley Orgánica 1/2015 incurre además en evidentes contradicciones al eximir de responsabilidad penal a los autores y coautores de los hechos, que no debería haber existido mediante la adopción y aplicación efectiva de los programas de cumplimiento adecuados para salvarlo de la pena, así como para recordar la limitación de la misma en el artículo 66 bis, los incumplimientos no críticos de las responsabilidades de supervisión, vigilancia y gestión mientras que el artículo 31 bis (b) simplemente toma en consideración los incumplimientos extremos de los deberes. Finalmente, la Ley Orgánica 2/2015, también de 30 de marzo, introduce una nueva modalidad de blanqueo de capitales en el artículo 576

del Código Penal español, con razón terrorista, que desvirtúa el interés jurídico legalmente protegido por medio de la criminalización del blanqueo de capitales, ya que no se exige que los productos utilizados para el terrorismo sean de origen ilícito.

Aunado a lo anterior, García (2018) expone en su artículo sobre el phishing como delito de estafa informática, la modalidad de estafa informática cuyo objeto principal es adquirir de los usuarios; i) claves, ii) números de cuentas bancarias con el propósito de obtener activos de forma ilícita esgrimiendo de forma falsa y fraudulenta identidades de terceros para captar los datos necesarios y ejecutar el fraude. Esta modalidad delictiva ha ido aumentando adoptando diferentes perfiles entre los que destaca el phisher-mule, en este sentido se han emitido pronunciamientos jurídicos que sopesan la responsabilidad de este nuevo perfil en la comisión del delito.

Ya que como asevera, Rodríguez (2015); el phisher-mule proporciona un aporte indispensable para la realización del fraude informático.

Flores (2014), en su artículo; Respuesta penal al denominado robo de identidad en las conductas de phishing bancario, la cual analizo la adecuación de los delitos contra la intimidad de su Código Penal para sancionar estas conductas, estableciendo la responsabilidad penal por la obtención de datos personales relativos a la identidad mediante el phishing. También, Flores (2013), en otro artículo titulado: La responsabilidad penal del denominado mulero o "phisher-mule" en los fraudes de banca electrónica; en el cual analiza la responsabilidad penal del este en los fraudes informáticos en línea, el blanqueo de capital incidiendo en el dolo.

Referente al banqueo de capital, Souto (2017); en su estudio: La expansión mundial del blanqueo de dinero y las reformas penales españolas de 2015, con anotaciones relativas a los ordenamientos jurídicos de Perú, Alemania, ecuador, los estados unidos y Méjico, hace referencia que el Perú el termino blanqueo se vinculó con el narcotráfico en el año 1991, con el paso de los años fue modificándose, y que atenta contra el principio de seguridad jurídica.

En un estudio en chile, de Oxman (2013), denominado: Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming", con relación al apoderamiento patrimonial; llego a la conclusión que el estado actual

de su legislación requiere una adecuada y rápida reforma para la punibilidad de estos fraudes informáticos, por lo que la obtención de datos personales online para la realización de transferencias de dinero no se puede tipificar en su Código Penal.

En el contexto nacional podemos mencionar las siguientes investigaciones:

Díaz (2019) analiza la aplicación de la ley Nº. 30096 Ley de Delitos Informáticos respecto a su regulación en el Derecho Penal Peruano, determinando la eficacia del reglamento mencionado en la Ley de ciberdelincuencia en cuanto a su regulación en el derecho penal peruano. Para lo cual se utilizó una cadena de estrategias de estudios cualitativos, de nivel descriptivo. Se empleó la encuesta como técnica y como instrumento la guía de entrevista. Logrando conclusiones específicas: el tratamiento de la delincuencia cibercriminal es inútil, dado que no existe una fiscalía especializada en ese tipo, generando inseguridad dentro de la investigación a nivel preliminar para que no siempre se ejecute una potente sanción de los delitos informáticos frente a los bienes delictivos incluidos dentro del reglamento único - Ley Nº. 30096.

En ese orden de ideas, Zorrilla (2018) en la investigación realizada sobre Inconsistencias y ambigüedades en la ley de delitos informáticos, Ley 30096 y su modificatoria Ley 30171, dichas inconsistencias han imposibilitado su eficaz cumplimiento, lo cual genera una visión sobre el desarrollo tecnológico y su afectación en casi todas las zonas del contexto social, donde siguieron una cadena de conductas ilícitas denominadas, genéricamente, "delitos informáticos". Por ello, los estudiosos del Derecho Penal han tratado de formular una percepción del delito que pueda servir para todas las instancias y en todos los lugares del mundo. El delito informático podría describirse como cualquier acción (movimiento u omisión) realizada con la ayuda de un ser humano que causa un daño a las personas sin beneficiar necesariamente al autor, al contrario, produce un beneficio ilegítimo a su autor, aunque ahora no lo haga a la vez o indirectamente perjudica a la víctima, tipificado con la ayuda de la Ley y se castiga con una pena. En esta experiencia, la generación de registros puede ser objeto de ataque o el método para cometer diferentes delitos. La generación de información tiene características muy diferentes para los estilos de delitos, principalmente de carácter patrimonial (estafa, apropiación indebida, etc.) con ayuda de terceros denominados mulas o mule. Las

conclusiones orientan la idoneidad proveniente de la gran cantidad de hechos recopilados con la facilidad para acceder a ellos y la especialmente manipulación de esos datos. La importancia más reciente de los sistemas de datos, debido a su impacto en el desarrollo de grupos, tanto públicos como privados, los ha convertido en un elemento cuyo ataque provoca un daño considerable, que va mucho más allá del coste material destruido.

En ese mismo contexto, Gallardo (2019) expresa como objetivo general determinar las modificaciones en la tipificación de delitos con la ratificación del convenio contra el cibercrimen en el Perú. Aplicó un estudio descriptivo. La principal conclusión se orienta a ratificar que es necesario modificar el Art 4° referido al "Atentado contra la integridad de sistemas informáticos" y la incorporación del delito informático de Falsificación Informática en el Capítulo referido a delitos contra la fe pública en la Ley N°30096 Ley de Delitos Informáticos, incluyendo el Dolo como agravante, enfatizando en el agente autor del delito como integrante de una organización criminal (phisher-mule).

Para referenciar el marco teórico se precisan las fuentes documentales que fundamentan la investigación, iniciando con la punibilidad. Méndez (2007) relaciona el término a toda conducta o comportamiento que tiene la posibilidad de aplicar a una pena o sanción sobre una infracción cometida por una persona, explícitamente menciona "es una categoría independiente aglutinante de todos los diversos presupuestos de la pena que están fuera de las anteriores categorías del delito y son ajenos a la culpabilidad, al tipo y a lo injusto" (p. 12). Igualmente, Vidaurri (2013) y Rincón & Giraldo (2020) afirman que es una consecuencia jurídica de un delito y las condiciones objetivas de la punibilidad (COP) son de carácter procedimental y no conforma un elemento configurador del cometido delito; por otro, lado Zorrilla (2020) y Frisch (2020) señalan que: las COP son condiciones desligadas a la acción típica, a excepción que el legislador las considere necesarias para aplicar la pena.

Otro aspecto a considerar son las condiciones objetivas de procedibilidad, en ausencia de las mismas no se obra contra el culpable, es decir, el hecho sigue siendo un inicuo penal y de renovarse el presupuesto procesal podrá perseguirse incluso produciéndose posterior al delito (Chirino y Giménez, 2019). De igual forma, las excusas absolutorias según Bermejo (2020) y García (2019) explican son

causas que aplican sobre un delito eliminando su punibilidad, obligando al juez a suprimir la sanción o pena de manera definitiva, considerándose; i) típica, ii) antijurídica y iii) culpable, es decir un delito es tentativo y consumado, pero al acogerse a la “excusa absolutoria” no existe merecimiento de pena.

Con base en lo anterior, la normativa tutelar de los delitos informáticos en el Perú se identifica como Ley Nº 30096 y tiene como objeto advertir y sancionar las conductas ilegítimas que afectan los medios y data electrónica, bienes jurídicos de preeminencia penal, cometidas a través de las tecnologías de la información y la comunicación (TIC), con el propósito de avalar la lucha efectiva contra la ciberdelincuencia (Congreso de la República del Perú, 2014). Para cumplir adecuadamente este propósito, en diciembre del 2020 se creó mediante resolución N° 1503-2020-MP-FN, de la Fiscalía de la Nación, la unidad Fiscal Especializada en Ciberdelincuencia, con lo cual se le dio un impulso jurídico al tratamiento de las modalidades delictivas de naturaleza digital, reformando la vocación de cumplimiento practico de la norma.

Un aspecto notable a resaltar de la presente investigación es el comportamiento del phisher-mule; considerando lo expuesto por Mayer (2018) estos son agentes intermediarios o terceros conocidos como “mulas” o “phisher-mule” que proporcionan sus datos bancarios a cambio de remuneración (de forma consciente o inconscientemente) para recibir dinero fraudulento, el cual posteriormente es transferido a un integrante de la banda delictiva. Los mismos no asumen las consecuencias de sus actos escudándose en el desconocimiento de la ley o del acto como tal, por desconocer la procedencia del capital transferido, presentando una conducta de inobservancia ante el delito perpetrado.

Del mismo modo, el bien jurídico protegido en los delitos informáticos vincula dos teorías, según Mayer (2017) la primera asume que este tipo de delito tutela un bien jurídico específico adjudicando un trasfondo de fondo y no de forma distinto a los tradicionales delitos y la segunda entiende: no tutelan un bien jurídico específico y "lo informático" no admite un argumento delictivo particular afectando la privacidad de los datos, el patrimonio y la fe pública. Por ende, los delitos informáticos y sus participantes no se diferenciarían de la trasgresión común en lo que incumbe a los intereses inmersos en el hecho, encontrándose un equilibrio

entre los delitos, destacando los bienes jurídicos tradicionales (directa o indirectamente) implantando ajustes legales para incluir el factor tecnológico (Brindis,2020).

Dentro de este marco, se encuentra el injusto típico a lo cual Mamani (2020) y Galindo (2017) aseveran que es la ejecución de un hecho típico acogido por una causal de justificación, por lo tanto, debe considerarse negado contrariamente a la autorización del justificante, pretendiendo impedir el hecho típico simbolizando una insuficiencia para inhibir el “derecho debido” a la lesión procedente.

Es conveniente resaltar, lo expuesto por García (2018) sobre la responsabilidad penal de los denominados "muleros", menciona que son personas que colaboran de manera consciente o inconsciente con los delitos informáticos y a través de los phishing, captando personas por internet específicamente por las redes sociales para después utilizarlas como intermediarios y transferir el patrimonio indebido. Estos muleros se quedan con un porcentaje del dinero como comisión por el trabajo realizado que finalmente es enviado a otras personas o entes privados.

En línea con esto, se han generado polémicas relacionadas con la atribución o no de responsabilidad criminal y penal por coadyuvar en la comisión del hecho punible, considerando que la conducta de los muleros se circunscribe intrínsecamente en el delito de fraude informático en su condición de cooperadores, otras doctrinas discurren; la conducta de los muleros se insertaría más en el “delito de receptación como ocultación” (Vilchez,2020). Tratando de evitar las investigaciones bancarias y la captación de estos puede aplicarse una vez ya se ha perpetrado el delito, derivando el concepto de "ignorancia deliberada" para estimar la presencia del dolo casual en la conducta de los muleros, justificando la jurisdicción de responsabilidad criminal.

Teniendo como comparación el Derecho Penal Español, el cual refiere según Leguizamón (2016), Que el problema se plantea para determinar si la mula puede ser culpable o no de estas acciones. El código penal español determina que para que una acción pueda ser constitutiva de delito, tiene que concurrir dolo o imprudencia. En estos casos, el dolo o intención no existe. La persona no es consciente de que está cometiendo un delito. Pero por lo general, los tribunales

españoles determinan que estas ofertas de trabajo tan bien remuneradas deberían llamar la atención del intermediario y este averiguar si realmente es un trabajo lícito. Por tanto, se considera que esta ignorancia deliberada no exime a la mula de la condena penal, y suelen ser condenados por cooperación necesaria o coautoría. Este tipo de condenas suele ser muy criticada ya que no se personaliza y estudia cada caso concreto, no se determina si el intermediario puede ser o no consciente de que se trata de un delito según sus capacidades y además algunos juristas opinan que el intermediario también es víctima del estafador. Pero por lo general, en España se condena la figura del intermediario y en algunas ocasiones, suelen ser bastante duros en las condenas. Se les suele condenar por delitos de blanqueamiento de dinero y receptación o estafas. Actualmente en España, hay muy pocas sentencias absolutorias a las mulas en los casos de phishing. Un ejemplo de una sentencia condenatoria en un caso de intermediario lo muestra la sentencia de la Audiencia Provincial de las Islas Baleares 264/2012.

Finalizando, consideramos los **enfoques conceptuales** los cuales permitieron analizar, profundizar y ahondar la presente investigación, teniendo, así como primera definición: **PHISHER- MULE:** es aquella persona que brinda su cuenta bancaria ya sea de forma consciente o inconsciente para la consumación del delito de fraude informático, percibiendo un porcentaje por dicho servicio prestado. **RECEPTACION:** en este caso lo consideraremos como la adquisición de un bien patrimonial de manera delictuosa. **IGNORANCIA DELIBERADA:** se refiere a la condición que asume una persona que debiendo conocer la naturaleza de un acto delictuoso, se da por no enterado. **CIBERFRAUDE:** es el delito que se comete mediante la utilización del internet.

Finalmente, luego de definir los enfoques conceptuales tenemos como un segundo aporte que se debería incentivar y reconocer el tema de la punibilidad del phisher-mule, ya que no contamos hasta el momento una buena legislación respecto al tema.

III. METODOLOGÍA

3.1 Tipo y Diseño de investigación:

El tipo de investigación es **básica**, ya que tuvo como objeto ampliar y ahondar conocimientos ya existentes del tema de investigación." es la búsqueda de ampliar nuevos conocimientos tanto científicos y culturales así como la innovación de nuevas tecnologías que nos permitirán el perfeccionamiento de los estados en la cual son el fin en este tipo de investigaciones" como lo manifiestan (Ñaupán, 2014, p. 135) . Por lo que esta investigación se ha buscado ampliar los conceptos e individualizar la responsabilidad del phisher-mule en los delitos informáticos. Respecto al diseño de investigación es **no experimental**; se aplicó la **teoría fundamentada**, "este es un método para construir teorías no deduciéndolas a partir de conceptos ya estudiados previamente por otros investigadores, sino induciéndolas, tomando como fuente de información fundamental la propia realidad" (Vargas, 2011, p.35). Por lo que se buscó recopilar información acerca de la punibilidad del phisher-mule, y de esta manera incrementar el contenido en nuestra ley ya existente en el Perú. Asimismo, aplica un **nivel descriptivo** según Ñaupas et al. (2014) referido a especificar las características, cualidades, propiedades, rasgos de los hechos y fenómenos de la realidad en un momento determinado.

3.2 Categorías, subcategorías y matriz de categorización.

Categoría 1: Punibilidad

Definición Conceptual: Mata (2020) asevera es un elemento del delito, que reside en el merecimiento de una penalidad, en función de la comisión de un delito; las mismas se establecen en el Código Penal de cada país.

Definición Operacional: representa la acción consecuencia de un hecho delictivo, la cual puede ser sentenciada o no, las subcategorías involucradas son: i) Condiciones objetivas de la punibilidad y el delito, ii) Condiciones objetivas de procedibilidad, iii) Excusas absolutorias

Categoría 2: Comportamiento del phisher-mule

Definición Conceptual**:** García (2018) conducta de los phisher-mule se circunscribe intrínsecamente en el delito de estafa informática en su condición de

cooperadores, otras doctrinas discurren que la conducta de los muleros se insertaría más en el delito de receptación como ocultación.

Definición Operacional: es el proceder de una persona como partícipe del hecho delictivo involucrando transferencia de fondos a través de cuentas bancarias personales a terceros fuera o dentro del territorio, donde se comete el fraude, resaltando que estos fondos son provenientes de delitos informáticos. Por lo tanto, se consideran las siguientes subcategorías; i) Conducta, ii) Bien jurídico protegido y iii) El injusto típico.

Tabla 1.
Contextualización de categorías y subcategorías.

Categoría	Definición Conceptual	Definición Operacional	subcategorías
Punibilidad	Mata (2020) asevera es un elemento del delito, que reside en el merecimiento de una penalidad, en función de la comisión de un delito; las mismas se establecen en el Código Penal de cada país.	Representa la acción consecuencia de un hecho delictivo, la cual puede ser sentenciada o no.	Condiciones objetivas de la punibilidad y el delito
			Condiciones objetivas de procedibilidad
			Excusas absolutorias
Comportamiento del mulero o phisher mule	García (2018) conducta de los phisher mule se circunscribe intrínsecamente en el delito de estafa informática en su condición de cooperadores, otras doctrinas discurren que la conducta de los muleros se insertaría más en el delito de receptación como ocultación.	Es el proceder de una persona como partícipe del hecho delictivo que involucra transferencia de fondos a través de cuentas bancarias personales a terceros fuera o dentro del territorio donde se comete el fraude, resaltando que estos fondos son provenientes de delitos informáticos.	Conducta
			Bien jurídico protegido
			El injusto típico

Fuente: Elaboración propia

3.3 Escenario de Estudio.

Es aquel contexto en el cual se realiza la investigación o donde se encuentran los datos que servirán de informantes para el objeto en estudio (Ramos, 2014)., en ese sentido, nuestro escenario se ubicó en el departamento y provincia del Cusco, recogiendo información de Profesionales en Derecho, especialistas en materia penal.

También se tuvo en consideración la documentación legal existente en Perú sobre la punibilidad del comportamiento del mulero o phisher-mule en derecho penal.

3.4 Participantes.

Los participantes a estudiar deben estar adecuadamente definidos, y pueden ser individuos, hechos, productos, procesos, grupos, instituciones o unidades de análisis de distintas naturalezas (Méndez, 2003). En consecuencia, los participantes de la actual investigación son: 10 Profesionales en Derecho.

Tómanos también como participantes fuentes de información de la normativa legal: i) Código Penal ii) Ley Nº 30096. y iii) Convención de Budapest.

Tabla 2.
Lista de entrevistados.

PARTICIPANTES	CARGO.
1. Abg. Jimmy Ray Chahuaylla Ccomanya.	Abogado Litigante.
2. Mag. Eloy Guillermo de la Sota Carazas.	Abogado Litigante/ Docente Universitario.
3. Abg. Héctor Fidel Machaca Alvaro.	Abogado Litigante.
4. Abg. Daniel Alcides Carrión Percca.	Abogado Litigante.
5. Abg. Darwin Bilbao Montesinos.	Abogado Litigante.
6. Abg. Yesica Cardeña Aybar.	Abogado Litigante.
7. Abg. Treicy Evelin Alba Aparicio.	Abogado Litigante.
8. Abg. Hugo Suni Quispe.	Abogado Litigante.
9. Abg. Teófilo Mengoa Coronado.	Abogado Litigante.
10. Dr. Enrique Jordán Laos Jaramillo	Dr. en Derecho/ Docente Universitario.

TOTAL:	**10 participantes.**

Fuente: elaboración propia.

3.5 Técnicas e instrumentos de recolección de datos.

En la recolección de datos; probamos la eficacia de una investigación; por lo cual hacemos uso de esta para poder describir el presente trabajo de investigación mediante el uso de la entrevista, de igual forma el análisis de documentos. Por lo que “El instrumento permite recopilar datos esenciales que nos servirá para nuestra investigación” (Nizama y Chávez, p.2020)

En este contexto, **la técnica de la entrevista**, “es una técnica de recolección de datos que nos permitió a que los especialistas en materia penal nos puedan dar su opinión frente al tema de investigación con las respuestas brindadas provenientes de la misma” (Hernández, Fernández y Baptista p403, 2014).

Por lo expuesto, el instrumento aplicado fue la **guía de Entrevista**. Dicho instrumento nos facilitó una información precisa y clara correspondiente a nuestro objetivo general y los objetivos específicos que se encuentran en la matriz de consistencia, debido a esto se desprende 9 preguntas brindadas al entrevistado, la cual se fracciono del problema general y los problemas específicos. De igual modo se aplicó la **guía de análisis documental**, consolidando la información y análisis respectivo de los hechos reales encontrados (Vargas, 2007, p.65).

3.6 Procedimientos.

Hernández et al., (2014) y Baena (2017) mencionan al respecto que no existe un esquema definido, puesto que hay actividades en paralelo, como es el caso de la aplicación y análisis del instrumento. Cada investigador puede definir su procedimiento. Por ello, se plantea; 1) indagar los datos, 2) imponerles una estructura (organizándose en unidades y categorías), 3) descubrir los conceptos, categorías, temas y patrones presentes en los datos, así como sus sujeciones, a fin de conceder la interpretación necesaria y explicarlos en función de la formulación del problema; 5) entender a profundidad el contenido que rodea a los

antecedentes, 6) reconstruir hechos e historias, 7) vincular los resultados con el conocimiento disponible y 8) generar una teoría fundamentada en los datos.

3.7 Rigor científico.

Representa la calidad de la investigación cualitativa, la cual debe estar encauzada a la certeza e integridad de la indagación, las mismas son determinadas por los investigadores, de tal manera que esta sea auténtica, convincente, creíble y honesta (Arias y Giraldo, 2011, p. 504). Así mismo la guía de entrevista fue validada por los siguientes expertos.

Tabla 3.
Tabla de validación de la guía de entrevista.

Datos Generales	Cargo	Condición	Porcentaje
Mag. Vargas Huamán Esaú.	Docente de metodología de investigación científica en la Universidad Cesar Vallejo.	Aceptable.	87%
Dr. Ludeña Gonzalez, Gerardo.	Docente de metodología de investigación científica en la Universidad Cesar Vallejo.	Aceptable.	93%
Mag. Santisteban Llontoq, Pedro Pablo.	Docente de metodología de investigación científica en la Universidad Cesar Vallejo.	Aceptable.	95%

Fuente: elaboración propia.

3.8 Método de análisis de la Información.

La presente investigación aplicó:

Método sistemático: permitiendo identificar situaciones, características o hechos del contexto jurídico que posibiliten el análisis completo a una determinada realidad (Clavijo et al.,2014)

Método Hermenéutico: son aquellas técnicas que se utilizan para el análisis de textos, permitiendo así comprender un determinado texto.

Método Interpretativo: es un método de investigación que nos ayudó a comprender toda la información obtenida mediante la guía de entrevista, al igual

que la guía documental; con resultados coherentes para la eficacia de la investigación.

Método Inductivo: es el procedimiento mediante el cual se reunió y analizo toda la información, para así obtener respuestas claras y precisas que resolvieron todas nuestras inquietudes.

3.9 Aspectos éticos.

Viera (2018) y Santi (2016) establecen que toda investigación tiene como objetivo formar a través de una serie de pautas y actividades inherentes a cada área de estudio, por ello debe cumplir con lineamientos éticos garantizando la imparcialidad, honradez y legitimidad de los datos analizados o recopilados. Considerando que los principios éticos de la investigación son internacionales y trascienden límites geográficos, económicos, legales y políticos; se establecen como aspectos éticos en la presente investigación respetar la confidencialidad de los datos recopilados, resguardar la identidad de los involucrados y sus opiniones, garantizar que las conclusiones y resultados sean manipulados solamente para fines académicos.

IV. RESULTADOS Y DISCUCIÓN:

En este numeral desarrollamos la descripción de los resultados recopilados en los instrumentos de recolección de datos como lo son la Guía de Entrevista y la Guía de Análisis Documental. En ese sentido, iniciamos exponiendo los datos recogidos de la Guía de Entrevista con relación al **Objetivo General**: **"**Determinar cómo el comportamiento del phisher-mule incurre en los delitos informáticos a la luz del derecho penal peruano", para ello formulamos las siguientes preguntas:

1.- De acuerdo a su experiencia, ¿cómo el comportamiento del mulero o phisher-mule configura el delito de fraude informático en el Perú?

2.- En su opinión, ¿cuál es la frecuencia con la que se cometen los delitos de fraude informático en el Perú?

3.- En su opinión, ¿de qué manera el avance tecnológico favorece el accionar del phisher-mule en la comisión del delito de fraude informático en el Perú?

Con referencia a la primera interrogante, Chahuaylla, De la Sota, Carrión, Bilbao, Cardeña, Alba, Suni, Mengoa, Laos (2021), refieren que el comportamiento del phisher-mule se configuraría en el delito de fraude informático de la siguiente manera, cuando este brinda su o sus números de cuentas bancarias ya sean nacionales o internacionales, para que de esta manera poder recibir las transferencias bancarias y así poder hacer movimientos libres de este dinero sustraído y este quedándose con un porcentaje del monto total sustraído; Por otro lado Machaca (2021), nos refiere que el phisher-mule es la persona que con su colaboración indispensable hace posible que se concretice el delito, por medio del uso del internet, afectando directamente el patrimonio de la víctima.

En ese entender, concebimos que el comportamiento del phisher-mule se da cuando este ayuda a su cómplice con la receptación del monto sustraído de manera ilícita, quedándose con un pequeño porcentaje de lo sustraído y el restante es depositado a cuentas extranjeras por entidades en los cuales dicha transferencia es muy difícil de rastrear.

Por otro lado, con referencia a la segunda interrogante, Chahuaylla, De la Sota, Machaca, Carrión, Bilbao, Cardeña, Alba, Suni, Mengoa, Laos (2021),

señalan que en la actualidad el incremento de la comisión de este delito se ha aumentado considerablemente, en un 12% en comparación con el año 2019, de esta misma forma, el año 2019, solo tuvo un incremento del 8% en relación al año 2018, Como lo refiere en su página oficial de la DIVINDAT. (DIVISION DE INVESTIGACION DE ALTA TECNOLOGIA).

Aunando a lo antes mencionado, tenemos que, con el desarrollo de la globalización veremos que va ir incrementando este tipo de delitos ya sea de forma progresiva o de forma acelerada.

Referente a la tercera interrogante, Chahuaylla, De la Sota, Machaca, Carrión, Bilbao, Cardeña, Alba, Suni, Mengoa, Laos (2021), manifiestan que gracias a la globalización que vivimos actualmente, los phisher-mule son contactados por medio del internet por los autores del fraude y estos generalmente son de países extranjeros.

Por ende, entendemos que mientras haya más avances tecnológicos aumenta la captación de los phisher-mule, logrando concretizar el fraude informático.

Respecto al **Objetivo Especifico 1:** "Analizar cuáles son los criterios legales existentes para la imputación penal del phisher-mule en los delitos informáticos en el Perú", se formularon las siguientes preguntas:

4.- De acuerdo a su experiencia, ¿cuáles son los criterios legales existentes para la imputación penal del phisher-mule en los delitos informáticos en el Perú?

5.- En su opinión, ¿cuáles serían o son las falencias que tiene la ley con respecto a los delitos informáticos en el Perú?

6.- De acuerdo a su experiencia, ¿de qué manera se podrían subsanar los vacíos legales existentes en la norma en cuanto a la imputación, en relación a los delitos informáticos?

Referente a la cuarta interrogante, Chahuaylla, De la Sota, Carrión, Bilbao, Cardeña, Alba, Suni, Mengoa, Laos (2021), nos manifiestan que en el Perú en la actualidad no existe criterios legales específicos que individualicen la imputación del actuar del phisher-mule en este tipo de delitos informáticos, sin embargo se

podría considerar o cabria el actuar dentro del delito de receptación; empero para Machaca (2021), refiere que se podría tomar en consideración los siguientes criterios como lo son la imputación objetiva a la conducta que sea típica, esto significa que este plasmado en el Código Penal, por así decirlo; pues así, de esa forma se pueda castigar al sujeto que incurrió en el delito, y la imputación subjetivo que viene a ser el resultado.

Así mismo, en respuesta a la quinta interrogante tenemos que, Chahuaylla, De la Sota, Machaca, Carrión, Bilbao, Cardeña, Alba, Suni, Mengoa, Laos (2021), manifiestan que en la Ley 30097 y su modificatoria la ley 30171, no se encuentra individualizada la tipificación con respecto al mulero, ya que esta se refiere de forma general con relación a los delitos informáticos.

De igual modo, en respuesta a la sexta interrogante tenemos que: Chahuaylla, De la Sota, Carrión, Bilbao, Cardeña, Alba, Suni, Mengoa, Laos (2021), señalan que debería aplicarse la analogía, haciendo uso de precedentes jurídicos, por otro lado Machaca (2021), nos pone en conocimiento que se deberían realizar un análisis exhaustivo de la jurisprudencia y proponer nuevos tipos penales y de esta manera se pueda sancionar con mayor severidad a los sujetos que incurran en los delitos informáticos e individualizar el accionar del phisher-mule.

Con respecto al **Objetivo Específico 2**: “Analizar cuáles son las implicaciones del comportamiento del phisher-mule en problemas relativos al dolo y la aplicación de la teoría de la ignorancia deliberada en el delito de estafa informática en el Perú”, se formularon las siguientes preguntas:

7.- De acuerdo a su experiencia, ¿cuáles son las implicaciones del comportamiento del phisher-mule en problemas relativos al dolo y la aplicación de la teoría de la ignorancia deliberada en el delito de fraude informático en el Perú?

8.- De acuerdo a su experiencia, ¿cuál sería el grado de participación del phisher-mule con respecto a la ignorancia deliberada en los delitos informáticos en el Perú?

9.- De acuerdo a su experiencia, ¿cree usted que el dolo por parte del phisher-mule podría considerase como agravante y de esta forma ser coautor en los delitos de fraude informático en el Perú?

Con referencia a la séptima interrogante tenemos que, Chahuaylla, De la Sota, Machaca, Carrión, Bilbao, Cardeña, Alba, Suni, Mengoa, Laos (2021), nos señalan que el dolo solo se aplica siempre y cuando la persona que haya colaborado con el delito de fraude informático tiene conocimiento pleno y toda la intención de cometerlo, por otro lado se considera que la ignorancia deliberada es utilizada por el mulero o phisher-mule, alegando que no tiene o no tenía conocimiento exacto o pleno de que estaba cometiendo el delito de fraude informático, esto se daría para evadir responsabilidades y por ende sanciones penales.

Con respecto a la octava interrogante se tiene que, Chahuaylla, De la Sota, Machaca, Carrión, Bilbao, Cardeña, Alba, Suni, Mengoa, Laos (2021), señalan que el mulero o phisher-mule para su propio beneficio se consideraría una víctima más, para de esta manera, este pueda evadir a la justicia, pudiendo alegar en su defensa que no tenía conocimiento pleno o consiente de la comisión del delito de fraude informático.

Para Finalizar, como respuesta a la novena pregunta tenemos que, Chahuaylla, De la Sota, Machaca, Carrión, Bilbao, Cardeña, Alba, Suni, Mengoa, Laos (2021), nos señalan con respecto al phisher-mule que si en su accionar interviene el conocimiento e intención se tendría que sancionar como autora y no simplemente como colaboradora, ya que va en perjuicio del patrimonio de la víctima.

Por lo tanto, se tiene por entendido para determinar si el phisher-mule actúa con dolo se debería de hacer una investigación preliminar exhaustiva, a cargo de la fiscalía especializada en delitos informáticos para recabar todas las pruebas necesarias y así tener la sanción correspondiente a su delito, y este no pueda apegarse a la ignorancia deliberada para disminuir o en tal efecto no sea penado.

De la **Guía de Fuente Documental**, con relación al **Objetivo General: "**Determinar cómo el comportamiento del phisher-mule incurre en los delitos informáticos a la luz del derecho penal peruano", se optó por analizar **El Código Penal Peruano Art. 196** del cual entendemos es un concepto genérico, con un

marco legal primario, para así de esa manera entender un poco más sobre delitos de defraudación. Ante ello tenemos la siguiente conclusión: El dispositivo legal abarca la definición de las conductas típicas que configuran el delito de estafa, básicamente en torno a los elementos penales clásicos de la estafa como lo son el lucro indebido para el que delinque y el consecuente perjuicio o daño perjuicio para la víctima.

De igual forma tenemos al **Objetivo específico 1: "**Analizar cuáles son los criterios legales existentes para la imputación penal de los phisher-mule en los delitos informáticos en el Perú", se optó por analizar el **Código Penal Peruano Artículo 196-A, numeral 5**, se puede considerar que este constituye la consagración penal de la Estafa en delitos informáticos.

Por otro lado, tenemos: lo que nos señala la **ley N° 30096 y su modificación, la ley N° 30171**, ambos contienen la tipificación sobre los delitos informáticos, a los que se define en orden especial de las conductas que realiza el sujeto pasivo para la obtención y aprovechamiento ilícito de los datos personales de sus víctimas.

Con respecto a lo anterior, tenemos las siguientes conclusiones; por un lado al Código Penal art. 196, numeral 5: tenemos que este aumenta los límites de la pena para las personas que incurren en estafa agravada, así como establece los elementos penales especiales de este tipo de estafa agravada como lo es la sustracción de datos para acceder a las tarjetas de debido o crédito de la víctima, y de la ley N° 30096 y 30171 concluimos que estas estipulan solo la modalidad de delitos informáticos o fraude informático y es contra el patrimonio.

Como consecuencia, observamos que tanto el Código Penal Peruano como la ley N° 30096 y su modificatoria N° 30171, se refieren a este tipo de delito de forma genérica, lo cual dificulta la tipificación e investigación plena del comportamiento de la figura del phisher-mule, del cual no se habla directamente y siento este la parte concluyente para finalizar el fraude informático de tipo phishing.

Es evidente que los avances tecnológicos posibilitan una nueva modalidad que no está totalmente definida en las leyes pero que son asumidos como estafa y que a su vez facilita cometer otros delitos contra las infraestructuras de información.

Para finalizar tenemos el **Objetivo Especifico 2:** “Analizar cuáles son las implicaciones del comportamiento del phisher-mule en problemas relativos al dolo y la aplicación de la teoría de la ignorancia deliberada en el delito de fraude informático en el Perú”.

Se optó por analizar el **Convenio de Budapest contra la Ciberdelincuencia**, este recoge las definiciones fundamentales sobre los delitos informáticos, de igual forma en el art. 8 inciso D señala “Cualquier forma de atentado al funcionamiento de un sistema informático, con la intención fraudulenta o delictiva, de obtener sin autorización un beneficio económico para sí mismo o para un tercero.

Del mismo modo, tenemos lo que es la **Jurisprudencia acerca de la Tesis de la ignorancia deliberada**, que señala que el autor de un delito no tenía intención de cometer el delito, se analiza su relación con los delitos de fraude informático. Por otro lado, la Jurisprudencia acerca de la tesis de la ignorancia deliberada concluimos que: Los encargados de la defensa de los procesados comúnmente recurren a alegar “ignorancia deliberada”. Esta doctrina en esencia se aparta de las exigencias para la imputación a título del dolo ofreciendo como solución la intencionalidad, que es relevante en el derecho penal. Se basa en que el sujeto provoca intencionalmente su ceguera, para facilitar su decisión moral, por lo tanto, el que realiza el hecho delictivo es tratado como ciego intencional al no querer saber nada.

En conclusión, de todas las guías documentales, nos damos cuenta que para la figura del phisher-mule no se encuentra individualizado para su correcta tipificación, ya que este se ve involucrado en la última fase del delito informático tipo phishing y en la mayoría de los casos se apegan a alegar ignorancia deliberada, para que no tengan la sanción correspondiente.

A continuación, en este apéndice redactamos la **discusión de resultados** de la investigación; Zorilla (2018) señala que esto se refiere a la inconsistencia y ambigüedades que existen en la Ley N° 30096 Sobre Delitos Informáticos y su modificatoria la Ley Nº 30171, lo que incide en imposibilitar su eficaz cumplimiento. Habida consideración de que la discusión es una comparación clave entre los

resultados de la investigación y los antecedentes, así como las teorías relacionadas con el tema, consideramos que los resultados derivados se pueden plantear de la siguiente manera:

De los resultados obtenidos en la Guía de entrevista con respecto al **Objetivo General:** Determinar como el comportamiento del phisher-mule configura el delito de Fraude informático a la luz del Derecho Penal Peruano, la mayoría de los expertos entrevistados especialistas en el derecho penal, sostienen que en la actualidad en el Perú no se encuentra tipificado en específico el comportamiento del mulero o phisher-mule en el código penal Peruano ya que estos son difícil de conceptualizar ya que se les puede ver como cooperadores y otros lo enfatizan en la receptación, por otro lado, también manifestaron un incremento considerable con respecto a la frecuencia con que se cometen los delitos de fraude informático en el Perú, en comparación a años anteriores, ya que en la actualidad vivimos en un mundo globalizado, y las personas exponen sus datos personales e información confidencias en el internet, dando mayor facilidad a que se cometa el delito de fraude informático.

Con referencia, a la información obtenida del **Análisis documental** del **Código Penal Art. 196,** solo se hace mención a la definición de Estafa en forma genérica, ofreciendo un marco legal primario para que de esta manera se comprenda los diferentes delitos de defraudación; no encontramos una tipificación que sancione el comportamiento del mulero o phisher-mule en el delito de fraude informático en el derecho penal peruano, juristas como Salinas (2015) observan que el delito de estafa se consuma cuando el sujeto haciendo uso de la astucia y el engaño induce al sujeto pasivo a fin de que este voluntariamente se desprenda y le entregue su patrimonio y obtener un beneficio indebido. Por lo tanto, entre los elementos de tipo penal de la estafa están el engaño y el daño, de allí que, la legislación debe enfocarse a reprimir dicha acción. En este punto es necesario analizar el principio de proporcionalidad que orienta al legislador cuando va aplicar la sanción que debe estar armonizada con el respeto de los derechos humanos.

Con relación a los antecedentes obtenidos de la investigación, Calderón (2021) en su artículo sobre la punibilidad del comportamiento del mulero, en el plantea una solución bajo qué tipo penal es punible la conducta del phisher-mule,

en la cual afirma que esta es punible como receptación y no como blanqueo de capitales, llegando a la conclusión que el phisher-mule no es ni autor ni cómplice.

Por otro lado, Guzmán (2003) señala que; Existen nuevas figuras que son típicas de haber sido cometidos utilizando maliciosamente las tecnologías de Información y comunicación, pero no son vistas como un derecho de la Información sino son subsumidas por otras disciplinas del Derecho cuyo cuerpo de leyes lo prevé y regulariza de manera más expresa, pero se debe más a la falta de conocimientos en estos temas de los propios legisladores.

En base al análisis de la **doctrina,** el autor Julio Mazuelos Coello en su libro "Modelos de Imputación en el derecho penal Informático" este refiere que a cada uno de los participantes del delito de fraude informático le corresponde una función o tarea distinta a la de los demás intervinientes, es decir, que cada uno ejerce por su lado un rol muy autónomo y estos a su vez son inherentes en el ejercicio de cada rol.

En conclusión, podemos observar que la conducta del phisher-mule no se logra establecer ni individualizar, mucho menos tipificar, por lo que se necesitaría realizar un estudio más profundo para su correcta tipificación e introducción en el código penal o le ley especial, por lo que se sugiere realizar un estudio más afondo de la conducta de este sujeto

Como segundo punto de discusión tenemos: el **Objetivo Especifico 1:** Analizar cuáles son los criterios legales existentes para la imputación penal del phisher-mule en los delitos informáticos en el Perú, la mayoría de los expertos entrevistados, sostienen que en la actualidad no existen criterios legales específicos para la imputación penal del phisher-mule en el Perú; sin embargo se podría considerar que el actuar del phisher-mule cabria dentro del delito de receptación; así mismo nos refieren que las falencias con respecto a la ley que se encuentra hoy vigente es que esta emitida de manera general y no de manera específica, por lo tanto no es posible sancionar al phisher-mule en el delito de fraude informático, y una manera de poder subsanar los vacíos legales existentes en la actualidad en la ley sería una modificatoria de la tipificación para la debida sanción del phisher-mule.

Por otro lado, teniendo en consideración las **Guías de Análisis Documental** señalan que:

Así la **Ley N° 30096**, en su artículo 8 modificado mediante **Ley Nº 30171**, que regula los delitos informáticos contra el patrimonio, el tipo penal citado resulta deficiente debido a que trata en el artículo 8 sólo la modalidad de hurto, sabotaje o estafa. Por lo tanto, la legislación no permite establecer una sanción efectiva para las acciones ilícitas; ya que dentro de esta figura de fraude arropa todos los posibles ilícitos. Siendo así, esta figura jurídica no tiene alcance debido a que no se cumple con el principio de tipicidad para sancionar el delito informático, resulta ser bastante genérica cuando pretende comprender todas las modalidades de delitos informáticos contra el patrimonio.

En este orden de ideas es poca la precisión legislativa en la Ley de Delitos Informáticos cuando no se ajusta a los hechos que deben ser sancionados. En la actualidad, se da una gran cantidad de delitos informáticos que no logran ser detectados debido a la sofisticación de las operaciones realizadas en la red negra. Por ejemplo, la Ley Nº 30096 y su modificación Ley Nº 30171 sanciona la alteración, borrado de datos o interferencia informática; donde la estafa no es comprendida en este rango, aunque sí, el sabotaje. En cuanto al hurto, no se aprecia una línea rectora que incluya esta modalidad, lo que lleva a contemplarla como intercepción de datos informáticos que está previsto en el artículo 7 de la ley mencionada.

El artículo 3 de la Ley 30096 prevé el atentado contra la integridad de datos informáticos, pero no tipifica esta ley en forma expresa el delito de sabotaje informático dificultando su penalización y prevención. Esto llevaría a pensar que la estafa informática tiene su razón de ser en la insuficiencia de la norma para hacerle frente a los casos de fraude donde no se lleva a cabo, ni engaño, ni el error y la disposición patrimonial la realiza el propio sujeto pasivo, así el defraudador extrae del sistema informático los datos de la víctima para usarlos en beneficio propio. De igual modo es útil destacar las limitaciones prácticas en las que el Estado peruano se encuentra para investigar y sancionar los delitos informáticos cometidos por personas en otros países, pero cuyo efecto recae en el país, lo cual es un evento bastante común, si tomamos en consideración la globalización de las redes y la ubicuidad de los sistemas informáticos en todos los órdenes de la vida común.

Así mismo, las limitaciones de la Ley inciden negativamente en la investigación y aplicación de sanciones. Sin embargo, los resultados del estudio muestran que, en el Perú, se revisó la ley 30096 en el 2013, razón por la cual se aprobó y modificó por la ley 30171 en el 2014, estando dicha modificación inspirada en los parámetros fijados por el Convenio de Budapest contra Ciberdelincuencia (2001) el cual entró en vigor en el país en el 2019.

Con relación a los **antecedentes obtenidos de la investigación**, Gallardo (2019), formula determinar las modificaciones de la tipificación de delitos con la validación del convenio contra el cibercrimen en el Perú. La principal conclusión, se orienta a ratificar que es necesario modificar el Art. 4 que se refiere al "atentado contra la integridad de sistemas informáticos" y la introducción del delito informático de falsificación informática en el capítulo que se refiere a los delitos contra la fe pública en la ley 30096.

Por otro lado, teniendo en cuenta el análisis de la doctrina, el autor Méndez (2020), en su libro Punibilidad y Delito, relaciona el término a toda conducta o comportamiento que tiene la posibilidad de aplicar a una pena o sanción sobre una infracción cometida por una persona, explícitamente menciona: "es una categoría independiente aglutinante de todos los diversos presupuestos de la pena que están fuera de las anteriores categorías del delito y son ajenos a la culpabilidad, al tipo y a lo injusto" (pág. 12).

No obstante, en el Derecho interno aún persisten fallas normativas para sancionar los delitos informáticos en especial los que afectan al patrimonio y que se siguen tipificando como fraude informático; sin contemplar la estafa, el hurto y el sabotaje.

En conclusión, en el Perú, se sanciona el acceso ilícito en el sistema informático, pero no hay un tratamiento claro del delito de estafa informática, el cual se reduce a la previsión del artículo 196-A, numeral 5, teniendo en consideración el Código Penal, que establece como estafa agravada, lo cual es muy llamativo, sobre todo si tomamos en cuenta que el delito de fraude informático implica la conexión con otras conductas criminales como la de phisher-mule, quien colabora activamente en la consumación del acto delictivo y del daño al patrimonio

de la víctima. En otras palabras, puede decirse que es un cooperador necesario sin el cual no se podría concretar o materializar el delito.

Como último punto de discusión, de los resultados obtenidos en la Guía de entrevista con respecto al **Objetivo específico 2:** "Analizar cuáles son las implicaciones del comportamiento del phisher-mule en problemas relativos al dolo y la aplicación de la teoría de la ignorancia deliberada en el delito de fraude informático en el Perú"; la totalidad de los entrevistados coinciden en que es muy difícil determinar y/o comprobar si hubo dolo o no en la comisión del delito de fraude informático en el Perú, ya que muchas veces los phisher-mule no tienen el conocimiento pleno de lo que se estaría realizando en la conducta delictiva, también señalaron que con respecto a la "ignorancia deliberada"; los phisher-mule muchas veces teniendo conocimiento o una ligera sospecha de que incurrirán en un delito estos prefieren darse por no enterados y de esta manera ponerse en situación de ignorancia deliberada.

Por otro lado, teniendo en consideración las **Guías de Análisis Documental** se tiene en cuenta que: El Convenio de Budapest es de las primeras y más completas iniciativas que en el marco del Derecho Internacional fue concebido para tratar de definir y abordar de forma sistemática la comisión de los delitos informáticos y, sobre todo, para lograr la concertación de los miembros de la comunidad internacional en la formulación de estrategias y políticas comunes, así como legislaciones uniformes, que permitieran la prevención y sanción de tales delitos a escala internacional. Recordemos que la altísima movilidad y ubicuidad de sistemas informáticos hace que un solo país resulte inerme ante ataques informáticos que pueden o no tener origen en su propio territorio, por lo tanto, la Convención de Budapest estableció todo un engranaje de colaboración, supervisión y mutua colaboración entre los distintos Estados signatarios, precisamente para evitar la evasión de la persecución penal. En ese sentido, se hizo importantes avances en materia de jurisdicción, manejo de datos en tiempo real; conservación, almacenamiento, etc.

En lo que respecta a **los antecedentes de la investigación**, de acuerdo con Mata (2020) y las condiciones de punibilidad del hecho cuando asegura que reside en el merecimiento de una penalidad que debe ir en función, de la comisión del

delito las cuales deben estar establecidas en el Código Penal respectivo. La función punitiva del Estado tiene límites al aplicar el principio de la proporcionalidad, pues debe existir coherencia cuando el legislador aplica las normativas legales.

Desde el punto de vista material objetivo, es el patrimonio el bien protegido y desde el punto de vista subjetivo se ampara el derecho que tiene su legítimo propietario a disponer de ese patrimonio del modo que mejor estime conveniente. Considerando que en la estafa priva el engaño y que la víctima obra por error, puede afirmarse que el delito lesiona también un importante derecho humano, como lo es la libertad. Así, en un delito informático como el *phishing* donde el error se induce a través de medios informáticos (como correos electrónicos, mensajes u otros idóneos) el delito no se materializaría sin la decisiva participación del *phisher-mule* quién actúa como factor decisivo y determinante para lograr que los fondos en dinero obtenidos ilícitamente, sean disponibles para el sujeto activo del delito electrónico.

Aquí, vale reflexionar acerca de la figura del phisher-mule, quién si bien no participa del proceso fraudulento de obtención de datos para el acceso a cuentas o instrumentos financieros, despliega una conducta de cooperación inmediata como receptor de fondos con el fin de a su vez de girarlos en favor del sujeto activo. Nótese, que esto supone un grado de coordinación muy alto y la existencia de acuerdo previo, a menudo simulado por una relación laboral, es decir, indicios de una organización criminal a gran escala que opera hacia y desde varios países. No es raro que el receptor último de los fondos ilícitos se ubique en países con una gran opacidad financiera, paraísos bancarios que permiten mantener el anonimato favoreciendo la continuidad de la actividad delictiva.

En correspondencia con lo planteado por Vilchez (2020), la conducta de los muleros se inserta en la del delito de receptación como ocultación, al tratar de evitar las investigaciones bancarias, alegando ignorancia deliberada para estimar la presencia del dolo y así justificar su conducta delictiva. El artículo 194 del Código Penal, si bien en principio pudiera señalarse alguna semejanza con la conducta del mulero, la especificidad del tipo penal consagrado para la receptación exige por un lado conocimiento del origen delictuoso y por otra parte está vinculado con un

objeto materialmente determinado. En otras palabras, no abarca típicamente el fenómeno en estudio.

Así mismo: Calderón (2021) señala que la ignorancia deliberada del resto del operativo o del delito no borra ni disminuye su culpabilidad, porque fueron conscientes de la antijuridicidad de su conducta. El hecho de asumir la teoría de la "ignorancia deliberada", en busca de beneficios procesales, no puede considerarse como un descargo válido, puesto que si bien es cierto que resulta imposible saber qué creía el sujeto en determinado momento, se puede deducir de su comportamiento la incurrencia en una conducta dolosa. Sin embargo, la ausencia de un sólido marco típico que facilite la persecución penal de los muleros, hace de la ignorancia deliberada un elemento con alta incidencia en las tesis de descargo.

En base a la **doctrina** utilizada, en el Perú, no existe definición legal para el dolo, pero sus alcances están delimitados; sin embargo, en los artículos 14 y 16 del Código Penal, se regula el error de tipo y la tentativa, de donde se desprende que el dolo, requiere como elemento indispensable el conocimiento, porque su ausencia excluye de responsabilidad penal. En este sentido hay importante jurisprudencia, como la emanada de la sentencia recaída en fecha 25 de julio de 2019, en el expediente 00740-2014-41-1903-JR-PE-04 de la Corte Superior de Justicia de Loreto, Segundo Juzgado Unipersonal de Maynas, puntos 1.3.3.3 y 1.3.3.4 del fallo, el cual deja establecido: "1.3.3.3. Con relación al conocer el origen ilícito ello nos conduce al dolo directo, normativizado por la teoría del rol, esto es, y siguiendo a la Casación 367-2011, Lambayeque, el cual ha señalado: "El problema de la prueba del dolo, será distinto en el caso de que el concepto sea de corte normativo. Ya no se buscará determinar el ámbito interno del procesado, sino que el énfasis se centrará en la valoración externa de la conducta, vale decir, en la imputación. En una concepción normativa del dolo, la prueba buscará determinar si el sujeto, según el rol que ocupaba en el contexto concreto, tenía o no conocimiento de que la acción que realizaba era constitutiva de un delito. 1.3.3.4. Por otro lado, está el poder presumirlo, el cual es entendida como la ignorancia deliberada, esto es, que el agente, deliberadamente, se auto coloque en una situación de no conocer un estado antijurídico, a fin de no verse perjudicado en sus propios intereses, pero que desde el rol que desempeña puede acceder al conocimiento del estado de

antijuridicidad, pero aun así persiste en querer desconocer; en efecto, y siguiendo a Ragués (2015), se puede identificar tres elementos que harían que la indiferencia deje el plano culposo y entre a configurar un delito doloso: a) Sospecha previa, b) Persistencia de la decisión de desconocer, c) Persecución de beneficios sin asunción de riesgos propios y evitación de responsabilidades. Por tanto, también actúa con dolo cuando el sujeto indiferente frente a su conducta lesiva, se guarda de riesgos que puedan poner en juego sus propios intereses".

Por otro lado, en el dolo el sujeto está consciente de lo que hace, es decir sabe que está haciendo la actividad riesgosa prohibida y también sabe que esta actividad tiene consecuencias dañosas y que teniendo conocimientos previos decidió hacerlo. Por lo tanto, en la ignorancia deliberada no se quiere advertir el riesgo del delito informático.

Así mismo, es importante señalar que la infección por malware y el acceso informático ilícito se consideran actos preparatorios para el phishing, de lo cual puede resultar la suplantación de identidad la cual es una conducta delictiva prevista en el artículo 9 de la Ley 30096 y está vinculado con el artículo 8 de la misma Ley, el cual establece el delito de fraude electrónico, que es la figura en la que encuadra el phishing en Perú. Declarativamente, la ley tiene como objetivo prevenir y sancionar acciones ilegales que afecten los sistemas, datos informáticos y otros activos jurídicos de relevancia penal mediante el uso de la tecnología con la finalidad de combatir la lucha contra los delitos informáticos. Por lo tanto, este tipo de delitos para el fraude informático sólo se admite como norma la condición objetiva de punibilidad del comportamiento deshonesto orientado hacia el provecho ilícito en perjuicio de un tercero motivado por el lucro indebido que debe comandar el inicio y desarrollo de la acción.

Del análisis concordante de estas normas especializadas y de la jurisprudencia nacional, cabe señalar que no hay una tipificación expresa y delimitada de la figura del *phisher-mule,* pero que estos, si son punibles bajo la figura de estafadores a los efectos sancionatorios del artículo 196 del Código Penal (y 196-A numeral 5 cuando aplique).

Existiendo a lo recopilado en el presente objetivo específico 2 concluimos que: los encargados de la defensa de los procesados comúnmente recurren alegar

“ignorancia deliberada”. Esta doctrina en esencia se aparta de las exigencias para la imputación a título del dolo ofreciendo como solución la intencionalidad, que es relevante en el derecho penal.

V. CONCLUSIONES:

Primero: Podemos observar que la conducta del phisher-mule no se logra establecer ni individualizar, mucho menos tipificar, por lo que se necesitaría realizar un estudio más profundo para su correcta tipificación e introducción en el código penal o le ley especial, por lo que se sugiere realizar un estudio más afondo de la conducta de este sujeto. En los últimos años la evolución tecnológica ha incrementado delitos como sabotaje informático, lavado de activos y fraudes. Ante esto se evidencia debilidad en la política asumida por el Estado peruano para la prevención, detección y sanción de estos delitos. En Perú se carece de organismos públicos sólidos que tengan niveles y mecanismos adecuados para luchar contra los delitos informáticos.

Segundo: En el Perú, se sanciona el acceso ilícito en el sistema informático, pero no hay un tratamiento claro del delito de estafa informática, el cual se reduce a la previsión del artículo 196-A, numeral 5, teniendo en consideración el Código Penal, que establece como estafa agravada, lo cual es muy llamativo, sobre todo si tomamos en cuenta que el delito de fraude informático implica la conexión con otras conductas criminales como la de phisher-mule, quien colabora activamente en la consumación del acto delictivo y del daño al patrimonio de la víctima. En otras palabras, puede decirse que es un cooperador necesario sin el cual no se podría concretar o materializar el delito. El sistema actual penal peruano presenta dificultades para prevenir, contrarrestar y sancionar los delitos informáticos. Problemas como la identificación física de la persona que cometió el delito, la falta de patrimonio de la persona natural para reparar los daños y la disolución de la responsabilidad penal en organizaciones bien estructuradas, no han sido solucionados de manera jurídica en el país.

Tercero: Los encargados de la defensa de los procesados comúnmente recurren alegar “ignorancia deliberada”. Esta doctrina en esencia se aparta de las exigencias para la imputación a título del dolo ofreciendo como solución la intencionalidad, que es relevante en el derecho penal peruano, de igual manera el principal problema para sancionar los delitos informáticos con relación al dolo y la ignorancia deliberada son la investigación y la sanción.

VI. RECOMENDACIONES

1.- Se recomienda al Congreso de la República, incluir en forma expresa en la legislación sobre los delitos informáticos contra el patrimonio, la diferenciación entre las modalidades de estafa, fraude, sabotaje o hurto informático, de igual manera al ente correspondiente la capacitación al personal de las fiscalías sobre el tratamiento y sanción del delito informático teniendo en cuenta el acelerado avance de la tecnología, el aumento en la perfección y cantidad de delitos informáticos y que son cometidos desde cualquier parte del mundo, limitando e imposibilitando la investigación y sanción de actos criminales.

2.- Se recomienda al Congreso de la República, una reforma legislativa con relación a la ley 30096 y su modificatoria 30171 de manera mucho más amplia y profunda, que, al incorporar nociones técnicas más precisas, permita no solo prevenir y sancionar los delitos informáticos contra el patrimonio, sino también abarcar otras figuras conexas con la comisión del delito, como el caso de los phisher-mule. La revisión frecuente de esta legislación especializada es importante puesto que todas las modalidades surgen como efecto de los acelerados avances tecnológicos.

3.- Se recomienda al Congreso de la República desarrollar con más profundidad la jurisprudencia de Perú, la Teoría de la Ignorancia deliberada; en relación con la cual, unificar criterios e integrar las más importantes corrientes doctrinarias, todo con el fin de evitar la evasión de sanciones y alcanzar los fines propios de la Ley, por lo que se recomienda analizar y comparar con el Derecho Penal Español ya que estos, se encuentra de manera más profundizada la doctrina con relación a los denominados phisher-mule.

REFERENCIAS

Arias, M. y Giraldo, C. (2011). El rigor científico en la investigación cualitativa. *Investigación y Educación en Enfermería*, 29 (3), 500-514. https://revistas.udea.edu.co/index.php/iee/article/view/5248/9829

Baena, G. (2017). *Metodología de la investigación.* Grupo Editorial Patria. México.

Bermejo, D. (2020). Análisis normativo de la regularización penal tributaria como excusa absolutoria. *Anuario de derecho penal y ciencias penales*, *73*(1), 601-641.

Brindis, M. (2020). El bien jurídico penal. *Alegatos*, *1*(31), 427-438. http://revistastmp.azc.uam.mx/alegatos/index.php/ra/article/view/1257

Calderón, L. (2021). La punibilidad del comportamiento del mulero o phisher-mule en derecho penal español. *Revista penal México*, 18 (1), 7-25. https://revistaciencias.inacipe.gob.mx/index.php/01/article/view/377

Calderón Tello, L. F. (2021). La punibilidad del comportamiento del mulero o phisher-mule en derecho penal español: análisis de la sentencia del tribunal supremo 834/2012 de 25 de octubre. *Revista Penal México*, *10*(18), 7-25. Recuperado a partir de https://revistaciencias.inacipe.gob.mx/index.php/01/article/view/377

|Chirino, L., & Giménez, M. (2019). Conducta criminal y su relación con la imputabilidad como elemento del delito. *Iustitia Socialis: Revista Arbitrada de Ciencias Jurídicas y Criminalísticas*, *4*(6), 28-51. http://dx.doi.org/10.4067/S0718-00122018000100159

Clavijo, D., Guerra, D., & Yáñez, D. (2014). *Método, metodología y técnicas de la investigación aplicada al derecho.* Grupo Editorial Ibáñez. Colombia

Cocchini, A. (2021). Los ciberataques de los actores no estatales y la “ciberdiligencia debida” de los estados. *Revista UNISCI/UNISCI Journal*, (55), 69-98. Doi: http://dx.doi.org/10.31439/UNISCI-106

Código Procesal Penal (2020). *Nuevo código procesal penal. Decreto legislativo nº 957.* Ministerio Publico. Fiscalía de la Nación. https://www.mpfn.gob.pe/elfiscal/nuevo_codigo/

Congreso de la República de Perú (2019). *Adhesión al Convenio de Budapest sobre Ciberdelincuencia*. (Consultado el 20 de febrero de 2021). https://static.legis.pe/wp-content/uploads/2019/09/Convenio-sobre-la-Ciberdelincuencia-Legis.pe_.pdf

Congreso de la República de Perú (2014). *Ley nº 30096*. (Consultado el 18 de febrero de 2021). https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1003117-1/

De la Mata, N., Dopico, J., Gómez, J., Lascuraín, J., & Nieto, A. (2018). *Derecho penal económico y de la empresa*. Editorial Dykinson. España.

Devia, E. (2017). *El delito informático: Estafa informática del artículo 248.2 del código penal*. (Tesis Doctoral, Universidad de Sevilla) Sevilla, España.

Díaz, C. (2019). *La aplicación de la ley Nº. 30096 -Ley de delitos informáticos respecto a su regulación en el derecho penal peruano.* (Tesis de pregrado, Universidad Cesar Vallejo). Lima, Perú.

Domínguez, J. (2020). *El blanqueo de capitales.* (Tesis de pregrado, Universidad de Valladolid) España. Uri: http://uvadoc.uva.es/handle/10324/42285

Ezu, G. (2020). Electronic Fraud and Performance of Deposit Money Banks in Nigeria: 2008-2018. *International Journal of Business and Management*; 15(6). DOI: https://doi.org/10.5430/afr.v8n2p202.

Flores, F. (2013). La responsabilidad penal del denominado mulero o "phisher-mule" en los fraudes de banca electrónica. *Cuadernos de política criminal,*110, 155-188. https://dialnet.unirioja.es/servlet/articulo?codigo=4476604

Flores, F. (2014) Respuesta penal al denominado robo de identidad en las conductas de phishing bancario. *Estudios penales y criminológicos,*34, 301-339 https://dialnet.unirioja.es/servlet/articulo?codigo=4888055

Frisch, W. (2020). Teoría de la pena, concepto de delito y sistema del hecho punible en transformación. *Revista de Estudios de la Justicia*, 32(1), 1-34. DOI: 10.5354/0718-4735.2020.57831

Gallardo, A. (2020). *Innovaciones en la tipificación de delitos con la ratificación del convenio contra el cibercrimen, en el Perú el año 2019*. (Tesis de pregrado, Universidad Científica del Perú). Loreto, San Juan Bautista, Perú).

García, A. (2019). *La excusa absolutoria en el Código Penal Peruano Cajamarca, 2018.* (Tesis de pregrado, Universidad San Pedro). Cajamarca, Perú.

García, D. (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(1), 650-661 http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2070-81572018000100025&lng=es&tlng=es.

Guzmán, M. (2003). Las tecnologías de información y comunicación en el derecho. *Revista Jurídica Cajamarca,* 13(1). https://www.derechoycambiosocial.com/RJC/Revista13/tecnologia.htm

Hernández, R., Fernández, C. & Baptista, P. (2014). *Metodología de la investigación*. Mc. Graw Hill. México.

Leguizamón, M. (2016). *El phishing, 2016.* (Tesis de grado en criminología y seguridad, Universidad pública Jaime I). Castellón de la Plana, España.

Mamani, R., & Mamani, E. (2020). *Eficacia del tipo penal de marcaje y reglaje en la reducción de delitos fin en el Perú.* (Tesis de pregrado, Universidad privada de Trujillo). URI: http://repositorio.uprit.edu.pe/handle/UPRIT/369

Mayer, L. (2017). El bien jurídico protegido en los delitos informáticos. *Revista chilena de derecho*, *44*(1), 261-285. Doi: http://dx.doi.org/10.4067/S0718-34372017000100011

Mayer, L. (2018). Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos. *Ius et Praxis*, *24*(1), 159-206. https://dx.doi.org/10.4067/S0718-00122018000100159

Mazuelos, J. (1). Modelos de imputación en el Derecho penal informático. *Derecho Penal Y Criminología*, 28(85), 37-54. Recuperado a partir de https://revistas.uexternado.edu.co/index.php/derpen/article/view/953

Méndez, C. (2003). *Metodología: diseño y desarrollo del proceso de investigación*. Sistema Librum 2.0. https://www.researchgate.net/publication/44349689

Méndez, E. (2007). *Punibilidad y delito.* Editorial Reus. España.

Molina, L. (2017). La realización de un hecho típico o del hecho positivo justificado no implica la infracción de la norma de determinación. *Verba luris*, (38), 81-89. Doi: https://doi.org/10.18041/0121-3474/verbaiuris.38.1054

Nizama, M., Chávez, L. (2020). *El enfoque cualitativo en la investigación jurídica, proyecto de investigación cualitativa y seminario de tesis.* Vol.38 Recuperada de: https://www.aulavirtualusmp.pe/ojs/index.php/VJ/article/view/1807/pdf08

Ñaupas H., Mejías, E., Novoa, E., & Villagómez, A. (2014). *Metodología de la investigación cuantitativa – cualitativa y redacción de tesis*. Ediciones de la U. Colombia.

Oxman, N. (2013). Estafas informáticas a través de Internet: acerca de la imputación penal del "phishing" y el "pharming". *Revista de derecho (Valparaíso)*, (41), 211-262. https://dx.doi.org/10.4067/S0718-68512013000200007

Palominos, G. (2020). ¿Imputación penal por el ámbito de organización de terceros?: el caso chileno de la responsabilidad penal de las personas jurídicas. *Revista Direito GV*, *16*(3). Doi: https://doi.org/10.1590/2317-6172201970.

Páramo, D. (2015). La teoría fundamentada (Grounded Theory), metodología cualitativa de investigación científica. *Pensamiento & Gestión*, 39(1),7-13. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1657-62762015000200001

Quinkert, F., Degeling, M., Blythe, J. & Holz, T. (2020) Be the Phisher -- Understanding Users' Perception of Malicious Domains.

ASIA CCS '20: The 15th ACM Asia Conference on Computer and Communications Security Taipei Taiwan October. *Association for Computing Machinery,* 263–276. Doi: https: //doi.org/10.1145/3320269.3384765

Ramos, C. (2014). *Cómo hacer una tesis de Derecho y no envejecer en el intento*. Ediciones Grijley. Lima, Perú.

Rincón, S., & Giraldo, J. (2021). Responsabilidad penal de las personas jurídicas en Colombia. *Tejidos Sociales*, *3*(1), 1-11.

Rodríguez, M. (2015) Estafa informática. El denominado phishing y la conducta del "mulero bancario": categorización y doctrina de la Sala Segunda del Tribunal Supremo. *Revista pensamiento penal*. http://revista.pensamientopenal.com.ar/fallos/42556-espana-estafa-informatica-denominado-phishing-y-conducta-del-mulero-bancario

Santi, M. (2016). *Ética de la investigación en ciencias sociales: un análisis de la vulnerabilidad en la investigación social*. Editor Globethics.net

Souto, M. (2017). Las reformas penales de 2015 sobre el blanqueo de dinero. *Revista electrónica de ciencia penal y criminología*, 19(1), 31. https://dialnet.unirioja.es/servlet/articulo?codigo=6243356

Souto, M. (2017). La expansión mundial del blanqueo de dinero y las reformas penales españolas de 2015, con anotaciones relativas a los ordenamientos jurídicos de perú, alemania, ecuador, los estados unidos y méjico∗. *Administración & cidadanía: revista da Escola Galega de Administración Pública*,12(2), 87-134. https://dialnet.unirioja.es/servlet/articulo?codigo=6525352

Thangavel, M., Yaamine, A. M., & Nandhini, J. T. (2021). Phishing Attacks in Mobile Platforms. In *Encyclopedia of Organizational Knowledge, Administration, and Technology Global IGI,* 1(1). 1228-1246. Doi: 10.4018 / 978-1-7998-3473-1.ch084

Vargas, X. (2011). *¿Cómo hacer investigación cualitativa?* Ediciones Etxeta. México

Vidaurri, M. (2013). *Teoría general del delito.* Oxford University Press México, S.A de C.V. México.

Viera, P. (2018). Ética e investigación. *Revista Boletín Redipe*, 7(2), 122-149. https://revista.redipe.org/index.php/1/article/view/434

Vílchez, R. (2020). La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional. *AIS: Ars Iuris Salmanticensis*, *8*(2), 21-25. Doi: 10.14201

Zorrilla, K. (2018). *Inconsistencias y ambigüedades en la ley de delitos informáticos ley nº 30096 y su modificatoria ley nº 30171, que imposibilitan su eficaz cumplimiento.* (Tesis de pregrado, Universidad Nacional de Ancash). Huaraz, Ancash, Perú).

ANEXOS.

ANEXO 1: MATRIZ DE CATEGORIZACIÓN DE APRIORÍSTICA.

NOMBRE DEL ESTUDIANTE:

Mariel Melissa Mengoa Valdivia.

Escuela profesional de derecho

AMBITO TEMÁTICO: Delitos Informáticos.

TÍTULO	
Punibilidad del comportamiento del phisher-mule en los delitos de fraude informático en el Perú.	
PROBLEMAS	
Problema General.	¿Cómo el comportamiento del mulero o phisher-mule incurre en delito informático a la luz del Derecho Penal Peruano?
Problema Especifico 1.	¿Cuáles son los criterios legales existentes para la imputación penal de los muleros en los delitos de fraude informático en el Perú?
Problema Especifico 2.	¿Cuáles son las implicaciones del comportamiento del mulero en problemas relativos al dolo y la aplicación de la teoría de la ignorancia deliberada?
OBJETIVOS	
Objetivo General.	determinar cómo el comportamiento del mulero o phisher-mule incurre en los delitos informáticos a la luz del Derecho Penal Peruano.
Objetivo Especifico 1.	Analizar los criterios legales existentes para la imputación penal de los muleros en los delitos informáticos en Perú
Objetivo Especifico 2.	Analizar las implicaciones del comportamiento del mulero o phisher-mule en problemas relativos al dolo y la aplicación de la teoría de la ignorancia deliberada.

SUPUESTOS	
Supuesto General.	que el phisher-mule no es una figura claramente establecida y delimitada en la consagración legal de los delitos informáticos a pesar que atentan contra el patrimonio de los particulares, lo cual pudiera corresponder a la errada o deficiente tipificación de la norma penal para esta clase de delitos.
Supuesto Especifico 1.	las condiciones de punibilidad en el derecho peruano son ambiguas, por existir distintas modalidades de fraudes informáticos y por el origen de los ataques virtuales, puesto que no necesariamente son cometidos por personas presentes en el país de la víctima.
Supuesto Especifico 2.	en la normativa peruana la sanción referida a la conducta de los muleros no está tipificada como tal, solo alude a ellos como participantes de delitos informáticos, en consecuencia, puede resultar una tipificación insuficiente para un delito que implica amplias consecuencias dañosas.
Categorización.	Categoría 1: **La Punibilidad.** Subcategorías 1: Condiciones objetivas de la punibilidad. Subcategorías 2: Condiciones objetivas de procedibilidad. Subcategorías 3: Excusas absolutorias. Categoría 2: **Comportamiento del phisher-mule.** Subcategorías 1: Conducta. Subcategorías 2: Bien jurídico protegido. Subcategorías 3: El injusto típico.
METODO.	

Diseño de Investigación.	**Enfoque:** Cualitativo. **Tipo de investigación:** Básica. **Nivel de la investigación:** Descriptivo. **Diseño:** Teoría Fundamentada.
Método de Muestreo.	**Escenarios de estudio:** Abogados y fiscales del departamento y provincia de Cusco con conocimientos en materia penal. **Participantes:** 10 Profesionales en derecho entre abogados y fiscales con conocimientos plenos en el tema Penal. **Muestra** no probabilística **Tipo:** De expertos Orientados por conveniencia
Plan de análisis y trayectoria metodológica.	**Técnica e instrumento de recolección de datos** **Técnica:** Entrevista y análisis documental. **Instrumento:** Guía de entrevista y guía de análisis documental: Código Penal, Ley Nº 30096. y Convención de Budapest.
Método de análisis de la información.	**Método:** sistemático, hermenéutico, analítico, interpretativo e inductivo.

ANEXO 4: INSTRUMENTO DE RECOLECCION DE DATOS.

GIUA DE ENTREVISTA.

(Abogados con conocimientos plenos en materia penal.)

Título: "Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú."

Entrevistado (a): ……

Cargo/ profesión/ grado académico: ……..……

Institución: ……..……

Objetivo General

Determinar cómo el comportamiento del phisher-mule incurre en los delitos informáticos a la luz del derecho penal peruano

1.- De acuerdo a su experiencia, ¿cómo el comportamiento del mulero o phisher-mule configura el delito de fraude informático en el Perú?

……
……
……

2.- En su opinión, ¿cuál es la frecuencia con la que se cometen los delitos de fraude informático en el Perú?

……
……
……

3.- En su opinión, ¿de qué manera el avance tecnológico favorece el accionar del phisher-mule en la comisión del delito de fraude informático en el Perú?

……

……

……

OBJETIVO ESPECIFICO 1

Analizar cuáles son los criterios legales existentes para la imputación penal del phisher-mule en los delitos informáticos en el Perú

4.- De acuerdo a su experiencia, ¿cuáles son los criterios legales existentes para la imputación penal de los muleros en los delitos informáticos en el Perú?

……

……

……

5.- En su opinión, ¿cuáles serían o son las falencias que tiene la ley con respecto a los delitos informáticos en el Perú?

……

……

……

6.- De acuerdo a su experiencia, ¿de qué manera se podrían subsanar los vacíos legales existentes en la norma en cuanto a la imputación, en relación a los delitos informáticos?

……

……

……

OBJETIVO ESPECIFICO 2

Analizar cuáles son las implicaciones del comportamiento del phisher-mule en problemas relativos al dolo y la aplicación de la teoría de la ignorancia deliberada en el delito de estafa informática en el Perú

7.- De acuerdo a su experiencia, ¿cuáles son las implicaciones del comportamiento del mulero en problemas relativos al dolo y la aplicación de la teoría de la ignorancia deliberada en el delito de fraude informático en el Perú?

……

……

……

8.- De acuerdo a su experiencia, ¿cuál sería el grado de participación del mulero o phisher-mule con respecto a la ignorancia deliberada en los delitos informáticos en el Perú?

……

……

……

9.- De acuerdo a su experiencia, ¿cree usted que el dolo por parte del phisher-mule podría considerase como agravante y de esta forma ser coautor en los delitos de fraude informático en el Perú?

……

……

……

_____

FIRMA Y SELLO

GUIA DE ANALISIS DE FUENTE DOCUMENTAL.

Título: “Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú.”

Autora:

Fecha:

Objetivos General.

Determinar cómo el comportamiento del phisher-mule configura el delito de estafa informática a la luz del derecho penal peruano.

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE A ANALIZAR	ANÁLISIS DEL CONTENIDO	CONCLUSIÓN

GUÍA DE ANÁLISIS DE FUENTE DOCUMENTAL.

Título: “Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú.”

Autora:

Fecha:

Objetivo Especifico 1

Analizar los criterios legales existentes para la imputación penal del phisher-mule en los delitos informáticos en Perú**.**

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE A ANALIZAR	ANÁLISIS DEL CONTENIDO	CONCLUSIÓN

GUÍA DE ANÁLISIS DE FUENTE DOCUMENTAL.

Título: “Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú.”

Autora:

Fecha:

Objetivo Especifico 2.

Analizar cuáles son las implicaciones del comportamiento del mulero o phisher-mule en problemas relativos al dolo y la aplicación de la teoría de la ignorancia deliberada en el delito de estafa**.**

FUENTE DOCUMENTAL	CONTENIDO DE LA FUENTE A ANALIZAR	ANÁLISIS DEL CONTENIDO	CONCLUSIÓN

ANEXO 5.

FICHA DE VALIDACIÓN

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: VARGAS HUAMÁN, Esaú

1.2. Cargo e institución donde labora: Docente y Asesor de Tesis de la Univeridad César Vallejo-Filial Lima.

1.3. Nombre del instrumento motivo de evaluación: Guía de Entrevista

II. Autora del Instrumento: Mengoa Valdivia, Mariel Melissa

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.										X			
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.										X			
3. ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la investigación.										X			
4. ORGANIZACIÓN	Existe una organización lógica.										X			
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales										X			
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.										X			
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.										X			
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos											X		
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.											X		
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.										X			

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación — SI
- El Instrumento no cumple con Los requisitos para su aplicación — -

IV. PROMEDIO DE VALORACIÓN : 87 %

Lima, 20 de marzo del 2021.

FIRMA DEL EXPERTO INFORMANTE
DNI No 31042328 Telf.: 963415453

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Ludeña Gonzáles Gerardo Francisco

1.2. Cargo e institución donde labora: Asesor y Docente de la Universidad Cesar Vallejo

1.3. Nombre del instrumento motivo de evaluación: **Guía de Entrevista**.

1.4. Autor de Instrumento: Mariel Melissa Mengoa Valdivia.

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales											X		
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.											X		

III. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación — SI
- El Instrumento no cumple con Los requisitos para su aplicación

IV. PROMEDIO DE VALORACIÓN: 93 %

Lima, 30 de Marzo.del 2021.

FIRMA DEL EXPERTO INFORMANTE
DNI Nº 28223439
ORCID: 0000-0003-4433-9471
RENACYT: P0103573 – Carlos Monge Medrano – Nivel IV

VALIDACIÓN DE INSTRUMENTO

V. DATOS GENERALES

5.1. Apellidos y Nombres: Santisteban Llontop Pedro

5.2. Cargo e institución donde labora: UCV

5.3. Nombre del instrumento motivo de evaluación: Guía de Entrevista.

5.4. Autor de Instrumento: Mariel Melissa Mengoa Valdivia

VI. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible.												X	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Este adecuado a los objetivos y las necesidades reales de la investigación.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Toma en cuenta los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÍA	La estrategia responde una metodología y diseño aplicados para lograr verificar los supuestos.												X	
10. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

VII. OPINIÓN DE APLICABILIDAD

- El Instrumento cumple con los Requisitos para su aplicación — SI
- El Instrumento no cumple con Los requisitos para su aplicación

VIII. PROMEDIO DE VALORACIÓN: 95 %

Lima, 30 marzo del 2021.

FIRMA DEL EXPERTO INFORMANTE

DNI No 0983311 Telf.: 987278657