FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima Norte 2022

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Abogado

AUTORA:

Barahona Rojas, Vanessa Josselin (orcid.org/0000-0002-1896-2529)

ASESOR:

Mg. Solano Arana, Vilder Marcelo (orcid.org/0000-0002-7258-328X)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal, Procesal Penal, Sistemas de Penas, Causas y Formas del Fenómeno Criminal

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA – PERÚ

2023

DEDICATORIA

El presente trabajo, lo dedico a mi madre, Doña María Dolores Rojas Janampa, que desde el cielo sé que se siente feliz y orgullosa por estos logros, a mis hijos Flavia y Fabiano los cuales han sido mi motivación para seguir adelante y mi hermana Sandra quien ha contribuido significativamente en diversas situaciones que atravesé, gracias.

AGRADECIMIENTO

Primer lugar, a Dios porque en este tiempo he gozado de salud, y ello me ha permitido desarrollar mis labores académicas; en segundo lugar, a mi madre, por siempre confiar en mí y ser un apoyo incondicional, que desde el cielo ella estará orgullosa de los logros obtenidos. Como tercer lugar a mi enamorado César, por ser aquella persona que siempre me motiva a continuar esforzándome para conseguir mis metas, y a mis docentes, por contribuir en mi etapa académica, con sus enseñanzas y experiencias que me han ayudado a desarrollar diversas habilidades cognitivas. Gracias

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, SOLANO ARANA VILDER MARCELO, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima Norte 2022", cuyo autor es BARAHONA ROJAS VANESSA JOSSELIN, constato que la investigación tiene un índice de similitud de 15.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 07 de Diciembre del 2023

Apellidos y Nombres del Asesor:	**Firma**
VILDER MARCELO SOLANO ARANA **DNI:** 09171502 **ORCID:** 0000-0002-7258-328X	Firmado electrónicamente por: VMSOLANOA el 09-12-2023 22:26:15

Código documento Trilce: TRI - 0687353

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Originalidad del Autor

Yo, BARAHONA ROJAS VANESSA JOSSELIN estudiante de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima Norte 2022", es de mi autoría, por lo tanto, declaro que la Tesis:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada, ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de la información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	**Firma**
BARAHONA ROJAS VANESSA JOSSELIN **DNI:** 47153602 **ORCID:** 0000-0002-1896-2529	Firmado electrónicamente por: VBARAHONAR91 el 17-12-2023 16:57:53

Código documento Trilce: INV - 1482926

INVESTIGA UCV

ÍNDICE DE CONTENIDOS

CARÁTULA i
DEDICATORIA ii
AGRADECIMIENTO iii
DECLARATORIA DE AUTENTICIDAD DEL ASESOR iv
DECLARATORIA DE ORIGINALIDAD DEL AUTOR v
ÍNDICE DE CONTENIDOS vi
ÍNDICE DE TABLAS vii
RESUMEN viii
ABSTRACT ix
I. INTRODUCCIÓN 1
II. MARCO TEÓRICO 4
III. METODOLOGÍA 10
3.1 Tipo y diseño de investigación 10
3.2 Categorías, subcategorías y matriz de categorización 10
3.3 Escenario de estudio 11
3.4 Participantes 11
3.5 Técnicas e instrumentos de redacción de datos. 13
3.6 Procedimientos 15
3.7 Rigor científico 16
3.8 Método de análisis de datos 16
3.9 Aspectos éticos 17
IV. RESULTADO Y DISCUSIÓN 18
V. CONCLUSIONES 32
VI. RECOMENDACIONES 33
REFERENCIAS 34
ANEXOS 39

ÍNDICE DE TABLAS

Tabla 1 Categorías y subcategorías 11
Tabla 2 Relación de participantes 12
Tabla 3 Validación de la Guía de Entrevista 14
Tabla 4 Tabla de validación de Guía de Análisis de Documentos 15
Tabla 5 Tabla de la Discusión de Objetivo General 25
Tabla 6 Tabla de la Discusión del Objetivo Específico 1 27
Tabla 7 Tabla de discusión del Objetivo Específico 2 29

RESUMEN

La presente investigación tiene como título “La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima Norte 2022” objetivo fue identificar los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir ciberdelincuencia Lima Norte 2022. Metodología considerada tuvo enfoque cualitativo, tipo fue básico, diseño fue fenomenológico y de corte transversal; donde el escenario de estudio fue Ministerio Publico- Fiscalía de la Nación, 2da Fiscalía Provincial Penal Corporativa de Carabayllo- Lima Norte Av. Tupac Amaru Km. 19, Mz B, Lt 13, AA. HH – El Dorado – Carabayllo con participación de cuatro (4) fiscales, dos (2) asistente en función fiscal y un (1) asistente administrativo pertenecientes a la fiscalía provincial Penal Corporativa De Carabayllo. Obteniendo como resultado que tipificación del phishing, ante la ocurrencia, generalización y evolución de este tipo de delitos cibernéticos en perjuicio de los ciudadanos, resultaría necesaria penalización, como mecanismo de prevención general en la ley 30096, debe de incorporándose los delitos de phishing, como otras modalidades como el pharming y carding con los que reducirán el índice de ciberdelincuencia en nuestro país. Concluyendo, que tipificación del phishing a pesar que existen leyes que sancionan como Ley 30096 y Ley 30171 (que la modifica) no son todos sancionados, debido que avance de tecnología se han ido originando nuevas maneras de cometer hechos ilícitos.

Palabras clave: Tipificación del phishing, ciberdelincuencia, sistema penal.

ABSTRACT

The title of this research is “The classification of phishing in our Peruvian criminal system, and the prevention of cybercrime, Lima Norte 2022”, the objective of which was to identify the legal foundations to classify phishing in the Peruvian criminal system to prevent cybercrime, Lima Norte 2022. Methodology considered had a qualitative approach, type was basic, design was phenomenological and cross-sectional; where the study setting was the Public Ministry- Prosecutor's Office of the Nation, 2nd Provincial Criminal Corporate Prosecutor's Office of Carabayllo- Lima Norte Av. Tupac Amaru Km. 19, Mz B, Lt 13, AA. HH – El Dorado – Carabayllo with the participation of four (4) prosecutors, two (2) tax assistants and one (1) administrative assistant belonging to the Carabayllo Corporate Criminal Provincial Prosecutor's Office. Obtaining as a result that classification of phishing, given the occurrence, generalization and evolution of this type of cybercrimes to the detriment of citizens, a penalty would be necessary, as a general prevention mechanism in Law 30096, phishing crimes must be incorporated, such as other modalities such as pharming and carding with which they will reduce the cybercrime rate in our country. In conclusion, the classification of phishing, although there are laws that sanction such as Law 30096 and Law 30171 (which modifies it), are not all sanctioned, due to the advancement of technology, new ways of committing illicit acts have been created.

Keywords: Typification of phishing, cybercrime, criminal system.

I. INTRODUCCIÓN

En la actualidad a nivel mundial las tecnologías de la información (TIC) han tenido un crecimiento exponencial en el uso de recursos, herramientas y programas debido al soporte del internet, con finalidad de administrar, procesar y compartir información a través de diversos equipos tecnológicos, como PC´s, laptops, teléfonos móviles, TV, entre otros, lo cual ha generado que existe una modalidad de configuración de acciones ilícitas que son conocidos como la Ciberdelincuencia y aprovechando que las personas deben usar muchas actividades dependiendo de un soporte tecnológico (Nuñez y Carhuancho, 2020).

Asimismo de acuerdo a Cámara (2020) en su investigación se enfocó en el nuevo delito moderno de criminología que es la Cibercriminología, donde se estudia que el perfil del delincuente es de un elevado conocimiento de la tecnología, siendo considerado un hacker y manejo del ciberespacio, donde menciona que estos ciberdelincuentes provienen de cualquier estrato social y diverso nivel socioeconómico. Del mismo modo, Acosta et al. (2020) en su investigación determinaron que los delitos informáticos, son reconocidos como actos ilícitos que se realizan por ciberdelincuentes usando la tecnología en forma inadecuada y dañando a terceras personas al obtener información privada de estas y usarlas en forma ilegal. Igualmente, Salvador (2022) consideraron en su investigación que a partir del año 2020 al aparecer la pandemia Covid-19 a nivel mundial, se incrementaron los ciberdelitos en el Ecuador, esto significo que los principales ciberdelitos que ocurren son la suplantación de identidad; falsificación y uso de documentos falsos, apropiación fraudulenta usando medios electrónicos.

Del mismo modo, en el contexto social peruano, el Diario El Peruano (2022) informo que cada año se siguen incrementando las denuncias de delitos informáticos debido a que solamente en el año 2021 recibieron 18,596 denuncia sobre el cibercrimen, lo que representa un incremento del 92,9% respecto al 2020. Igualmente, en otro reporte del Diario El Peruano (2022) informo que la región Lima es la que tiene mayores índice con 7,234 casos, seguidos de Arequipa con 877 casos, La Libertad con 835 casos y la región Callao con 774 casos.

Considerando a Zelada (2021) menciono en su investigación, que la ley 30096 sobre delitos informáticos busca prevenir y a la vez sancionar este tipo de acciones

ilícitas que afectan los sistemas y datos de empresas jurídica y personas naturales. Por lo que plantean que la ley debe ser más amplia y considerar que los delitos cibernéticos son formas nuevas de criminalidad, la cual debe de tener una pena acorde a la acción criminal que realizan.

Debemos de indicar que la problemática de nuestra investigación es que la ley 30096 no considera la tipificación del delito informático del phishing, debido a que en la actualidad los delitos informáticos se han incrementado en forma exponencial, afectando a miles de usuarios a nivel nacional a partir del año 2020 en plena pandemia, como se ha indicado que la Región Lima ha tenido 7,234 casos de los denuncias**,** por eso es importante en la presente investigación se ha realizado un análisis de la actual situación de este delito**,** la propuesta que sea tipificado y ha sido sustentado mediante encuestas a expertos como son abogados especialistas en el tema de ciberdelincuencia, además de considerar la información de reportes a nivel internacional sobre Ciberseguridad año 2021, información adicional del Poder Judicial y Ministerio Público.

La pregunta de investigación del **problema general**, ¿Cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima norte 2022? De igual forma, el **problema específico1**, ¿Cuáles serían aquellos elementos que se deben de tener en cuenta para tipificar la conducta delictiva del phishing para la prevención de ciberdelincuencia Lima norte 2022? Y el **problema específico 2**, ¿Cuál sería la naturaleza jurídica que se debe considerar para tipificar la conducta delictiva del phishing como prevención de ciberdelincuencia Lima Norte 2022?

La justificación teórica del presente estudio tuvo como necesidad tipificar en el delito del phishing, en el actual sistema penal peruano debido que la ley N°. 30096 sobre los delitos informáticos y su reciente modificatoria N°. 30171, no contemplan ni regula este acto ilícito que se efectúan en el sistema informático apropiándose de información privada y usándola para fines delictivos, por eso la investigación es importante el incorporar al phishing en la ley 30096 con finalidad de hacer una lucha directa contra la ciberdelincuencia en el país y reducir los riesgos que afecta a la sociedad, al no estar tipificada. **La justificación práctica**, se consideró al análisis toda la información obtenida de las entrevistas a realizar a los abogados sobre el tema de la investigación, con finalidad de detallarse los

resultados de la misma y su posterior análisis. **La justificación metodología**, fue de tipo de aplicada porque ha tenido en cuenta la teoría considerada sobre la ley 30096, delitos informáticos e información del Ministerio Público, será del tipo fenomenológico debido a que la información obtenida no ha sido modificada y será cualitativo, debido a que se aplicó la entrevista para obtener información de expertos en ciberdelincuencia para enriquecer el desarrollo de la investigación.

En la investigación se plantea como **objetivo general**, Identificar los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima Norte 2022. Del mismo modo, el **objetivo específico 1** Identificar los elementos que se deben de tener en cuenta para tipificar la conducta delictiva del phishing para la prevención de ciberdelincuencia Lima Norte 2022 y el **objetivo específico 2** Determinar la naturaleza jurídica que se debe considerar para tipificar la conducta delictiva del phishing como prevención de ciberdelincuencia Lima Norte 2022.

Finalmente, se tuvo los supuestos de investigación, **el supuesto general**, los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia, por otro lado, el **supuesto especifico 1**, elementos relevantes de carácter penal tomados en cuenta para tipificar la conducta delictiva del phishing confines de prevenir la ciberdelincuencia en Lima Norte 2022 y el **supuesto especifico 2**, naturaleza jurídica que se debe considerar para tipificar la conducta delictiva del phishing como prevención de ciberdelincuencia Lima Norte 2022.

La contribución del presente estudio, que debido a ser un tema de actualidad sobre el phishing usado por la ciberdelincuencia, se debe de dar un aporte para que la Ley 30096 sea aplicada de forma correcta, por lo que se consideran las entrevistas a participantes como aporte de la investigación y de los autores de investigaciones nacionales e internacionales, como aporte académico.

La relevancia en presente estudio, es la importancia de la Ley 30096 sobre los delitos informáticos como debe tipificarse en nuestro sistema penal peruano, para sancionar adecuadamente a los delincuentes cibernéticos, que a través de acciones inescrupulosas afectan a usuarios al robar su identidad, usufructúan sus documentos, valores e información confidencial.

II. MARCO TEÓRICO

A continuación, se detallan antecedentes internacionales para sustentar la investigación se ubica a los autores Bhavsar et al. (2018) en su artículo realizaron un estudio sobre el ataque del phishing en la sociedad, por eso considera que el phishing es uno de esos tipos de metodologías que se utilizan para adquirir la información. El phishing es un delito cibernético en el que se dirigen correos electrónicos, teléfonos, mensajes de texto, información de identificación personal, datos bancarios, datos de tarjetas de crédito y contraseñas. El phishing es principalmente una forma de robo de identidad en línea. Concluye, que su trabajo de investigación da una idea justa del ataque de phishing, los tipos de ataque de phishing a través de los cuales se realizan los ataques, la detección y la prevención.

Por otro lado Piña (2019) en su artículo enfocó como la ciberdelincuencia en México se ha multiplicado especialmente por el desarrollo de las herramientas tecnológicas de la información, que las entidades bancarias y comerciales han desarrollado con finalidad de promocionar sus productos y servicios, y que estas son aprovechadas por organizaciones criminales que a través de malware y spam sorprenden a las personas, con lo cual utilizan los datos de otras personas y afectando su economía y reputación. Concluyeron, que es importante que México trate de acogerse a la Convención de Budapest que establece un marco jurídico con respecto a los delitos informáticos.

A la vez, Ortiz (2019) en su investigación indicó que los delitos informáticos en Ecuador han aumentado exponencialmente, debido a que las organizaciones criminales que usan el mundo virtual, han logrado crecer en el desarrollo de ingresar a empresas y de personas, debido a que el desarrollo tecnológico le permite desarrollar diversos programas malware para poder ingresar en dispositivos y sistemas informáticos con finalidad de intervenir en el sistema de empresas y en cuentas de personas. Asimismo, concluye que debe de existir un programa de capacitación virtual para que las personas puedan evitar sufrir robo de su identidad y que le roben sus datos personales.

Asimismo, Patayo (2021) en su investigación efectuada, consideró que el phishing es una actividad fraudulenta que atenta contra las personas al usar en

forma ilegal su identificación. Los ataques de phishing conducen a la pérdida de dinero, reputación, trabajo, etc. Se han realizado muchas investigaciones al respecto y se han puesto a disposición muchas soluciones, pero los piratas informáticos aún encuentran y desarrollan nuevos métodos para engañar a las medidas de seguridad vigentes. Concluyendo, que el phishing en la actualidad se moderniza en nuevos desarrollos técnicos, con lo cual sorprenden a las personas al robar su identificación personal.

Asimismo, Sviatun et al. (2021) consideraron en su investigación que el cibercrimen amenaza la seguridad nacional de diferentes países del mundo. El crecimiento de los ciberataques desestabiliza el orden internacional y trastorna el normal funcionamiento de las relaciones internacionales. Su propósito del artículo académico es analizar las causas y las consecuencias económicas del nivel de ciberdelincuencia en el mundo e identificar los arreglos legales modernos para combatir la ciberdelincuencia. Establecieron que el nivel de ciberdelincuencia en el mundo y las consecuencias económicas de su impacto tienden a aumentar. Se estima que en 2020 el costo total del cibercrimen y la ciberseguridad superará el billón de dólares estadounidenses.

Asimismo, Castañeda et al. (2021) su artículo tuvo por finalidad el analizar los delitos cibernéticos en los paises de México, Colombia y Chile para que puedan estudiar los ordenamientos jurídicos de estas nuevas formas de delitos y ver los avances con respecto al Convenio sobre Ciberdelincuencia 2001 firmado en Budapest. Concluyeron, que los países involucrados a la fecha tienen leyes que sancionan la ciberdelincuencia, pero no aplican de acuerdo a lo requerido por la Convención sobre la Ciberdelincuencia que ocurre en Chile y México, porque no han modernizado su legislación para una sanción más tipificada a los nuevos instrumentos de delincuencia cibernética como son el phishing, smishing, vishing, entre otros.

Por otro lado, Devanny et al. (2022) en su artículo señaló que el inició del poder cibernético en la competencia interestatal se aborda con frecuencia en la literatura académica sesgada hacia los poderes globales, comúnmente pasando por alto poderes regionales que gobiernan en Brasil. El artículo abordó esta brecha al investigar cómo los cibernéticos el poder es concebido e implementado por actores gubernamentales brasileños. Determina sobre el análisis de datos

primarios relativos a la documentación de políticas de Brasil y marco institucional. El artículo comienza con una visión más amplia del ciberpoder. e investiga su relación con la ciberdefensa y la seguridad, iluminando la comprensión brasileña actual del ciberpoder como una herramienta operativa dentro del ámbito militar.

Asimismo, Macías et al. (2022) determinaron en su investigación, que los delitos informáticos a nivel mundial y en el Ecuador se han incrementado en forma exponencial a partir del año 2020, donde se menciona en los periódicos, revistas, noticias de radio y programas periodísticos que los casos más numéricos son la suplantar identidad, falsificar documentos, entre otros. Todos estos casos son relevantes en la sociedad ecuatoriana, y las leyes establecidas no han reducido los mismos, debido a que los ciberdelincuentes no tienen temor a sus acciones ilegales que realizan, debido a que sus métodos cada vez son más desarrollados y difíciles de ubicar.

Asimismo, Alcalá y Meléndez (2023) explicaron claramente en su investigación que la transformación digital ocurrida en el mundo por el desarrollo del internet, del uso de nuevas herramientas móviles de conexión virtual han conducido a una gran transformación de las actividades bancarias, comerciales, laborales, educativa y demás, hacia una digitalización a nivel mundial. Como ocurre en México, estas herramientas llevaron al origen de organizaciones criminales denominadas ciberdelincuencia que aprovechando este desarrollo tecnológico realizan acciones delincuenciales con transmisión ilícita de datos y afectan en las personas su intimidad, imagen, honor, entre otras y principalmente sustraer información bancaria afectando su economía.

Asimismo, De La Torre y Quiroz (2023) su investigación la iniciaron a raíz de la pandemia Covid19 y el desarrollo de herramientas tecnológicas como un soporte tecnológico para el buen funcionamiento de la comunicación entre clientes y entidades bancarias y entre bancos y empresas comerciales, y viceversa. De este desarrollo tecnológico aparecieron organizaciones fraudulentas que, a través del ciberespacio, crean programas o malvare (software maliciosos), para ingresar en equipos móviles o sistemas informáticos para obtener información y utilizarse en su beneficio propio, al suplantar identidades y perjudicar económicamente a las personas y empresas. Concluyendo, que la ciberdelincuencia se ha incrementado 300% en Venezuela tres años anteriores.

Se describen **antecedentes nacionales** que sustentan la investigación para lo cual se ubicó a los autores: Pichihua (2020) en su artículo publicado en el diario Andina virtual mencionó que a partir año 2019 se registraron 3,012 denuncias de fraudes electrónicos, suplantación de identidad y otro delitos cibernéticos, esta cifra se ha elevado en 8% con respecto al año 2018, dentro del total existieron 1,641 denuncias por usurpación de personas en transacciones por internet, 431 casos de compras fraudulentas con tarjetas de crédito y 25 denuncias de clonación de tarjetas. Concluyendo, que los principales fraudes electrónicos se han desarrollado con el phishing, con lo que los delincuentes cibernéticos engañan a las víctimas en conseguir su contraseña e ingresar a sus cuentas, asimismo mediante enlaces maliciosos o páginas webs falsas de entidades bancarias.

Por otro lado, Riega et al. (2021) en su artículo llegaron a la conclusión después que han analizado las leyes correspondientes contra la ciberdelincuencia en los países de América Latina, indicaron que existen leyes contra este nuevo delito, pero que no sancionan adecuadamente a nuevas acciones delincuenciales como phishing, smishing, vishing, estas no se encuentran tipificadas en sus respectivas leyes y no se complementan con el Convenio sobre Ciberdelincuencia realizado en la ciudad de Budapest el año 2001, es por eso que mencionan que en la actualidad la ciberdelincuencia sigue creciendo y afectando los intereses de empresas y personas.

Por otro lado, Vinelli (2021) en su artículo consideraron que debido al incremento de las operaciones comerciales virtuales que se aplican desde equipos móviles y el uso de monederos digitales, esta evolución ha generado la aparición de organizaciones criminales que mediante diversos procesos cibernéticos ingresas a las cuentas de empresas, instituciones y personas, cometiendo suplantación de identidad. A pesar que existe la ley 30096 esta ley no tipifica al phishing como delito y los criminales no son sancionados, por lo que concluyó, que el Estado Peruano debe de modificar la ley contra debilitos cibernéticos y que esta tenga tipifica sanciones adecuadas contra estas modalidades delictivas.

Asimismo, Leyva (2021) en la investigación que realizó consideró como objetivo establecer la realidad jurídica con finalidad de tipificar los delitos informáticos en el Perú. La ley Nº 30096 no es clara al respecto, se debe de modificar la ley y considerar las nuevas herramientas ilegales desarrolladas para

ser tipificadas con penas de cárcel, sustentadas por la inseguridad ciudadana actual que han generado estas organizaciones cibernéticas criminales que afectan los intereses informáticos de las instituciones en el país.

Al respecto, Ramírez et al. (2022) su investigación realizada fue determinar conciencia en estudiantes universitarios, sobre la identificación de los principales indicadores sobre los cibercrímenes en nuestra sociedad y enumerarlos de acuerdo a su importancia, la muestra fue de 372 estudiantes mediante encuestas por Google Form, las respuestas son: 1) conciencia sobre phishing, 2) conciencia sobre el spamming, 3) eficacia del software antivirus, y 4) bullying en la web. Concluyeron, que los estudiantes universitarios tienen conocimiento de los modelos de cibercrimen que existen, y consideran que la sociedad debe ser capacitada ante los engaños fraudulentos de estas organizaciones dirigidas por criminales con alto conocimiento de sistemas.

Respecto a las teorías relativas al tema, Benavides et al. (2020) el phishing es conocido como una combinación de ingeniera y exploits técnicos, a través de los cuales convencen a las personas en proporcionar sus claves o datos personales para acceder a sus diversas cuentas personales en entidades bancarias, financieras y comerciales. El procedimiento de un hacker que utiliza el phishing tiene el siguiente proceso: (i) enviar un enlace al email personal de una persona con un enlace (url), (ii) este URL lo deriva a una web falsa y (iii) finalmente el phisher ya tiene acceso al manejo de la cuenta de la persona. Del mismo modo, Hernández y Baluja (2021) como Calvo (2022) menciona que el phishing es calificado como un sistema de ataques a cuentas bancarias de personas, que son engañadas y que a través de Bancos y cajas, entre otras usan varias modalidades de ciberdelincuencia pata afectar a los usuarios de entidades financieras, bancarias y comerciales.

De acuerdo a la teoría de ciberdelincuencia, Santos y Teixeira (2020) mencionaron que como todos sabemos el ciberespacio se ha ampliado para todos los servicios de las empresas y personas debido al desarrollo de herramientas tecnológicas que efectúan un movimiento elevado de conexiones diarias a nivel mundial. De este crecimiento se han aprovechado organizaciones criminales para afectar a los que usan estos servicios, para robar identidades para sustraerles dinero y datos para usos ilegales, a este acto criminal virtual se le llama “Ciberdelincuencia”. Del mismo modo, Parada y Errecaborde (2018) mencionaron

que la ciberdelincuencia en unos de los actuales fraudes financieros que se han incrementado, debido al mayor movimiento de transacciones comerciales bancarias y promociones de servicios y servicios dirigidos a sus clientes, quienes son sorprendidos por delincuentes cibernéticos que mediante el phishing obtiene sus datos y hurtan de sus cuentas bancarias sus fondos disponibles. Igualmente, Cámara (2020) donde menciona que la ciberdelincuencia se trata de una criminología especializada en el impacto de las tecnologías digitales en forma negativa a diversos usuarios para aprovecharse de sus cuentas bancarias y realizar estafas.

Finalmente, como **enfoque conceptual** de la investigación en el Perú se aprobó la Ley 30096 (2013) denominada ley de delitos informáticos y modifica en algunos artículos en la ley 30171 publicada en marzo del 2014, la cual se encuentra relacionada sobre Convenio sobre la Ciberdelincuencia de Budapest del año 2001. La ley 30096 claramente se enfoca en tipificar los delitos informáticos contra datos y sistemas informáticos, indemnidad y libertad sexuales, contra la intimidad y secreto de las comunicaciones, contra el patrimonio y la fe pública, pero no considera la tipificación con nombre propio del phishing.

De acuerdo al derecho comparado, sobre phishing en América, los países que han aprobado en sus respectivos congresos leyes para enfrentar la ciberdelincuencia, como en Chile año 1993 Ley No. 19223, Colombia año 2009 Ley No. 1273, Argentina año 2008 Ley No. 26388 y en el Perú año 2013 Ley No. 30096, quienes de acuerdo a Jiménez (2021) detallan que en América Latina las estafas a través del ciberdelincuencia llega a niveles de los $30,000 millones de dólares anuales, por eso los países se reúnen para analizar estrategias para enfrentarlos.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

3.1.1. Enfoque y tipo de investigación

Para la presente investigación el enfoque fue de tipo cualitativa, debido que se considera la tipificación del phishing en el sistema penal peruano, según Baena (2017) lo define cuando el investigador describe, interpreta y entiende los resultados obtenidos, con la finalidad de poder interpretar información obtenida.

El tipo de investigación considerado fue básico, que según Sánchez et al. (2018) es cuando se encuentra orientada a la búsqueda de nuevos conocimientos, con la finalidad de incrementar los conocimientos científicos.

3.1.2. Diseño de investigación

El diseño considerado ha sido fenomenológico, de acuerdo a Hernández et al. (2017) se considera cuando la información obtenida no será modificada ni alterada en beneficio del investigador, del mismo modo será de corte transversal, La Madriz (2019) es cuando la información obtenida corresponde a un solo periodo, en este caso en el año 2023.

3.2 Categorías, subcategorías y matriz de categorización

Se logro una mejor orientación en nuestro tema de investigación, resultando fundamental el reconocimiento y la clasificación de las categorías y subcategorías pertinentes. Esto nos permitió profundizar en el estudio del tema y analizar los resultados de manera más precisa y completa.

Por lo tanto, están estrictamente relacionadas con los problemas y objetivos de estudio de la matriz de categorización.

Tabla 1

Categorías y subcategorías

Categorías	*subcategorías*
Categoría 1: Tipificación del phishing en el sistema penal peruano	(1) Ley No. 30096 - Delitos informáticos. (2) Proceso judicial: casos de ciberdelincuencia.
Categoría 2: Prevención de ciberdelincuencia,	(1) Administración de Justicia (2) División de Investigación de delitos de Alta Tecnología.

Nota: elaboración propia (2023)

En relación a la matriz de categorización se localiza en el anexo 1.

3.3 Escenario de estudio

De acuerdo a Cabezas et al. (2018) lo define como aquel territorio o lugar en el cual se va a realizar el estudio, el cual se encuentra limitado según el alcance de la investigación., por lo tanto, como escenario se fue la fue Ministerio Publico-Fiscalía de la Nación, 2da Fiscalía Provincial Penal Corporativa de Carabayllo- Lima Norte Av. Tupac Amaru Km. 19, Mz B, Lt 13, AA. HH – El Dorado – Carabayllo

3.4 Participantes

Según Hernández et al. (2017) la muestra es considerada una parte de la población, que tienen iguales características, con finalidad de obtener información para su posterior análisis. En tal sentido estuvo conformada por: cuatro (4) Fiscales, dos (2) Asistente en Función Fiscal y un (1) asistente Administrativo especialistas en el tema de ciberdelincuencia, además ha sido completado con información adicional del Poder Judicial y Ministerio Público.

A continuación, se detalla los nombres de los participantes.

Tabla 2

Relación de participantes

N°	APELLIDO Y NOMBRE	PROFESIÓN O GRADO	CARGO	INSTITUCIÓN	EXPERIENCIA
1	Méndez Navarro Juan Manuel	Magister en Derecho Penal	Fiscal Provincial	2da fiscalía provincial Penal Corporativa de Carabayllo	10 años
2	Víctor Alberto Mendoza Robles	Magister en Derecho Penal	Fiscal provincial	2do fiscalía provincial penal corporativa de Carabayllo – 1er Despacho	10 años
3	Traverso Poma Richard Alexander	Magister en Derecho Penal	Fiscal Adjunto	2da fiscalía provincial Penal Corporativa de Carabayllo	5 años
4	Deyda Soto Rojas	Magister en Derecho penal	Fiscal Adjunto	2da fiscalía Provincial Penal Corporativa de Carabayllo	10 años
5	Cajo Palacios Roxana Elizabeth Genesis	Licenciada en Derecho	Asistente de Función Fiscal corporativa de	2da fiscalía provincial Penal	5 años

			Carabayllo – 2do Despacho	Corporativa de Carabayllo	
6	Núñez Choquehuanca Raquel Laura	Licenciada en Derecho	Asistente de Función	2do fiscalía provincial penal corporativa de Carabayllo – 1er Despacho	5 años
7	Darwin Darío Cari Huacachi	Licenciado en Derecho	Asistente Administrativo	2da Fiscalía Provincial Penal Corporativa de Carabayllo 2do Despacho	5 años

3.5 Técnicas e instrumentos de redacción de datos.

Asimismo, la técnica usada fue el análisis documental, definida por Baena (2017) que es obtener una serie de documentos relacionados con la investigación y las variables planteadas, con finalidad de evaluarlos y definir mediante tablas, gráficos y resúmenes, de la información obtenida y analizada para beneficio del desarrollo de la investigación.

Asimismo, la otra técnica que se aplico fue la entrevista que se realizó a participantes definidos, que son cuatro (4) fiscales, dos (2) asistentes en función Fiscal y un (1) asistente administrativo, especialistas en el tema de ciberdelincuencia, según Sánchez et al. (2018) la entrevista es una técnica en una

investigación que tiene por finalidad obtener información básica para el estudio la cual es estructurada debido a que se prepara en forma ordenada considerando las dimensiones establecidas.

Asimismo, respecto al instrumento se usó la guía de análisis documental, según Durán (2018) la lista de cotejo o guía de observación es aquella donde se detallan todos los documentos necesarios del Poder Judicial y Ministerio Público.

Del mismo modo se empleó como instrumento la guía de entrevista, es el cuestionario, según Hernández et al. (2017) como un instrumento en una investigación con una seria de preguntas relacionadas con el tema de las investigaciones definidas para obtener información para desarrollo del estudio.

Tabla 3

Validación de la Guía de Entrevista

Validación de la guía de entrevista		
Validador	**Cargo**	**Condición**
Agustín Nicolás, Arosemena Angulo	Docente: Universidad César Vallejo	Aceptable
Levi Joel, Aguirre Rojas	Docente: Universidad César Vallejo	Aceptable
Ubaldo, Callo Deza	Docente: Universidad César Vallejo	Aceptable

Fuente: Elaboración propia (2023)

De acuerdo a Peña (2022) el análisis de fuente documental, la define como un proceso que significa verificar los contenidos de los documentos para su comprensión y se identifiquen la relevancia de acuerdo a la investigación que es está realizando.

Asimismo, la ficha de análisis documental de acuerdo a Sánchez et al. (2018) es un documento en el cual se describen todos aquellos documentos necesarios para una investigación, para su verificación y posterior uso.

Tabla 4

Tabla de validación de Guía de Análisis de Documentos

Validación de Instrumento - Ficha de Análisis de documento	Datos Generales	Mg. Vilder Marcelo Solano Arana	Condición
	Cargo	Docente Metodólogo de Investigación UCV	Aceptable

Fuente: Elaboración propia (2023)

La guía de entrevista se localiza en el anexo 2

3.6 Procedimientos

El procedimiento tuvo como objeto el tratamiento de análisis que sostiene como propósito responder al problema planteado, por consiguiente, la presente investigación responde al enfoque cualitativo basado en teorías fundamentales, la investigación se desarrolló sobre la base de recaudar datos que se obtuvieron a partir de un análisis documental, con la totalidad de la información adquirida de los estudios de los diferentes autores internacionales y nacionales, libros y revistas científicas, elementos que contengan el marco teórico y se aplicaron a la guía de análisis documental. Asimismo, se recabaron los datos de recolección de información que ha brindado los diferentes participantes expertos en la presente investigación. Por otro lado, se ha recabado información de análisis documentos obtenidos del Ministerio Público y Poder Judicial.

Por consiguiente, se efectuó la coordinación con cada uno de nuestros participantes abogados y personal especializado, para el desarrollo de nuestra entrevista, con la finalidad de obtener los resultados que contestaron a los objetivos planteados en la presente investigación.

3.7 Rigor científico

Se basa en la calidad de la investigación y se da mediante los criterios de calidad: Credibilidad, que según Erazo (2018) se utiliza un software para verificar la similitud como el Turnitin, con el cual se verifico la similitud de la presente investigación. Transferibilidad, para Erazo (2018) es el objetivo de investigador en logar obtener información de otros investigadores con finalidad que sirva como sustento en nuestra presentación. Seguridad, para Erazo (2018) se utiliza con finalidad que todas las fuentes sean citadas según normas APA. La Confiabilidad, para Erazo (2018) es tener en cuenta de acuerdo a las entrevistas a realizarse a los expertos, debido a que ellos cuentas con la experiencia para poder sustentar la presente investigación.

Asimismo, dado que la disciplina científica exige una cuidadosa evaluación de la confiabilidad y calidad de la investigación, se decidió solicitar la validación de los datos de este estudio cualitativo a tres profesionales en lo que respecta a investigación. Se utilizo el instrumento de recolección de datos, específicamente la guía de entrevista, se llevó a cabo una exhaustiva revisión para garantizar su adecuación y pertinencia.

3.8 Método de análisis de datos

Se considera a toda la información recibida, la cual fue analizada y ordenada, lo mismo que las entrevistas realizadas, este método ha sido el hermenéutico, que según Quintana y Hermida (2019) es un proceso que tienen en primer lugar analizar e interpretar las fuentes o textos incluidos en una investigación, para posteriormente realizar la parte interpretativa.

De acuerdo a Cabezas et al. (2018) el método inductivo es considerado como científico, el cual se deriva en conclusiones generales a partir de premisas individuales, para lo cual se recolectan los datos específicos.

En la triangulación se utilizó el método hermenéutico que de acuerdo a Feria et al. (2019) es cuando se refiere al uso de varios método en una investigación, que pueden el hermenéutico e inductivo, en sus fuentes de datos recopilados, teorías, antecedentes de teóricos para el desarrollo de la investigación.

3.9 Aspectos éticos

La presente investigación consideró los valores éticos que la Universidad César Vallejo (UCV) plantea en sus políticas y procedimientos, del mismo modo se respetó el uso de investigaciones de autores terceros y los mismos se encuentran citados según la norma APA establecida. Asimismo, se tiene en cuenta que se cumplió con obtener información y el desarrollo de la misma se encuentra dentro de los porcentajes de similitud que la universidad exige.

Adicionalmente, la investigación desarrollada cumple la resolución de Vicerrectorado de Investigación Nº 062-2023-VI-UCV, donde se detalla la guía de elaboración de trabajo que conducen a grados y títulos de los estudiantes que desarrollan estas investigaciones.

IV. RESULTADO Y DISCUSIÓN

Se desarrollo en el presente capítulo los resultados de las entrevistas realizados a cuatro fiscales, dos asistentes en función fiscal y un asistente administrativo destacados en la fiscalía provincial Penal Corporativa De Carabayllo, a través de los cuales se ha obtenido información importante para su análisis y tratamiento.

Respecto al **objetivo general** se tiene en cuenta lo siguiente: “Identificar cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima Norte 2022”. Resultados obtenidos por parte de nuestros expertos (participantes):

De la **primera pegunta** que se ha planteado en la guía de entrevista efectuada se tiene lo siguiente: A su criterio ¿Considera usted que los delitos del phishing deben ser incorporados y penalizados en nuestro sistema de justicia?, para lo cual respondieron: Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Núñez (2023) y Traverso (2023) afirmaron, con el avance de la tecnología se han ido originando nuevas maneras de cometer hechos ilícitos, tal como phishing, que es una forma de fraude en línea que implica engañar a las personas, haciéndose pasar por instituciones confiables, a fin de obtener información confidencial de las tarjetas de crédito, tal como las contraseñas, números de tarjetas y demás detalles, siendo que dichos actos ocasionan daños financieros y personales a las víctimas, lo que ocasiona que las personas pierdan la confianza en las transacciones que se hacen a través del internet, además la totalidad de los participantes expertos mencionan que el artículo 207-A no cumple con las premisas de incluir todas las modalidades de la delincuencia virtual.

De la **segunda pregunta** que se ha planteado en la guía de entrevista efectuada se tiene lo siguiente: A su criterio ¿Cuáles serían los elementos objetivos que deben ser considerados a fin de tipificar dichas conductas?, para lo cual respondieron: Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Núñez (2023) y Traverso (2023) afirmaron, que para que se configure el delito phishing, se debe tener presente los siguientes elementos objetivos: i) Suplantación de identidad, es decir, el autor del evento delictivo debe hacerse pasar por una entidad confiable tal como un banco u otra organización gubernamental. ii) Engaño o

Fraude, esto es, la simulación de situaciones o sucesos de hechos materiales y psicológicos, para inducir a error a su víctima, pero dicho engaño debe ser idóneo o suficiente. iii) Medios electrónicos, los cuales deben ser utilizados para llevar a cabo el engaño en la víctima, como por ejemplo correo electrónico, página web, mensaje de texto u otro medio. iv) Obtención de la Información, aquí es cuando se consuma el delito mencionado, pues a través de los otros elementos antes mencionados, el autor del hecho ilícito logra obtener las contraseñas, cuentas de ahorro, los números de tarjeta, los usuarios entre otros. v) Daño patrimonial, es causado a consecuencia de la entrega de la información, ya que dicha información permite realizar los fraudes, hurto u otro delito.

De la **tercera pregunta** que se ha planteado en la guía de entrevista efectuada se tiene lo siguiente: En su opinión ¿Considera que es importante la tipificación de las modalidades como el Phishing, en nuestro ordenamiento jurídico?, para lo cual respondieron: Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Nuñez (2023) y Traverso (2023), afirman que es muy importante poder tipificar la comisión del delito de phishing, ya que va a permitir delimitar de manera clara las acciones que van a constituir el delito en mención, orientando a las autoridades del Poder Judicial, Ministerio Público y Policía Nacional del Perú poder investigar y perseguir los casos de phishing, facilitando la cooperación entre estas autoridades para luchar contra el crimen cibernético, asimismo, dicha normativa va a disuadir a los autores de este tipo penal, permitiendo así la protección a la víctima.

Análisis e interpretación de las categorías emergentes

De acuerdo al objetivo general: Identificar cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima Norte 2022.

En desarrollo de la presente investigación, se ha podido apreciar la aparición de categorías emergentes debido por información obtenida por parte de los entrevistados, que se consideran de importancia, para evaluar y discutir puntos determinantes para entender de la mejor manera nuestra investigación. Por lo tanto, de acuerdo al objetivo general, es muy importante poder tipificar la comisión del delito de phishing, que debe permitir delimitar las acciones que van a constituir el delito en mención, orientando a las autoridades del Poder Judicial, Ministerio

Público y Policía Nacional del Perú poder investigar y perseguir los casos de phishing, debido que actualmente los ciberdelincuentes están incrementando sus delitos debido al incremento de la tecnología se han ido originando nuevas maneras de cometer hechos ilícitos, caso del phishing y otras modalidades.

Análisis de las fuentes documentales

Referente a las fuentes documentales indicadas en el objetivo general, de acuerdo a Zelada (2021) en su investigación "Delitos informáticos ¿Nuevas formas de criminalidad?" explica que presupuestos especiales de delitos informáticos permiten relacionar sobre la criminalidad económica, que no solamente se circunscribe a delitos patrimoniales, sino que también engloba tipos penales que cuentan con una importante repercusión en el sistema informático y, accesoriamente, en el sistema económico. Del mismo modo, Castañeda et al. (2021) en su investigación "Vista de los delitos cibernéticos en Chile, México y Colombia" mencionaron que los países involucrados a la fecha tienen leyes que sancionan la ciberdelincuencia, pero no aplican de acuerdo a lo requerido por la Convención sobre la Ciberdelincuencia que ocurre en Chile y México, porque no han modernizado su legislación para una sanción más tipificada a los nuevos instrumentos de delincuencia cibernética como son el phishing, smishing, vishing, entre otros.

Respecto al **primer objetivo específico** se tiene en cuenta lo siguiente: Identificar cuáles son los elementos a considerarse para tipificar la conducta delictiva del phishing para prevenir la ciberdelincuencia Lima Norte 2022. Para lo cual se realizaron las siguientes preguntas:

De la **cuarta pregunta** que se ha planteado en la guía de entrevista efectuada se tiene lo siguiente: En base a su experiencia ¿Qué naturaleza jurídica debe adoptar la tipificación de las conductivas del Phishing, de resultado o peligro?, para lo cual respondieron: Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Nuñez (2023) y Traverso (2023), afirman, que la naturaleza jurídica del phishing, es de resultado, porque al obtener la información confidencial de las tarjetas de crédito débito, otras cuentas de ahorros u otra información personal y/o financiera, se configura el delito en mención, ya que después de obtener dicha

información, lo que queda es el perjuicio patrimonial a la víctima, por lo que, el resultado especifico es esencial para que el delito se considere completo. Por último, el resultado del phishing no solo se refiere a la obtención de información, sino también a las posibles consecuencias negativas para la víctima, como la pérdida financiera y el riesgo de robo de identidad.

De la **quinta pregunta** que se ha planteado en la guía de entrevista efectuada se tiene lo siguiente: En base a su experiencia diga usted ¿Cuáles son las modalidades más frecuentes en el Perú, para la comisión del delito de fraude informático?, para lo cual respondieron: Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Núñez (2023) y Traverso (2023), afirman que las modalidades serian en primer término, las páginas clonadas falsas, a través del phishing, donde las ciberdelincuencias engañan a los usuarios con paginas falsas que simulan ser los sitios web de los bancos o entidades financieras. En segundo; termino, las compras fraudulentas, donde los bancos o entidades financieras. En segundo; termino, las compras fraudulentas, donde los ciberdelincuentes ofertan productos online, donde se falsifican ofertas o descuentos de reconocidas tiendas en línea, acción que lesiona cada vez más frecuentes a través de mensajes de texto o notificaciones donde se acceden a sitios web clonados.

De la **sexta pregunta** que se ha planteado en la guía de entrevista efectuada se tiene lo siguiente: A su criterio ¿La ciberdelincuencia se incrementa debido a falta de una ley adecuada?, para lo cual respondieron: Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Núñez (2023) y Traverso (2023), afirman, en primer término, por la falta de diligencia de los usuarios de plataformas web, y segundo, por la ausencia de información de las redes involucradas en estas actividades que deberían tener plataformas de web más seguros y difundir las modalidades usadas por los ciberdelincuentes. Luego es la necesidad de una regulación preventiva y ulteriormente y una regulación punitiva como exige la población.

Análisis e interpretación de las categorías emergentes

De acuerdo al objetivo específicos 1: Identificar cuáles son los elementos a considerarse para tipificar la conducta delictiva del phishing para prevenir la ciberdelincuencia Lima Norte 2022.

Con respecto al primer objetivo específico, es importante considerar que, los elementos a considerarse en la tipificación del delito del phishing, que para que se configure el delito phishing, se debe tener presente los siguientes elementos objetivos: i) Suplantación de identidad, es decir, el autor del evento delictivo debe hacerse pasar por una entidad confiable tal como un banco u otra organización gubernamental. ii) Engaño o Fraude, esto es, la simulación de situaciones o sucesos de hechos materiales y psicológicos, para inducir a error a su víctima, pero dicho engaño debe ser idóneo o suficiente, entre los más importantes a señalar.

Análisis de las fuentes documentales

Referente a las fuentes documentales indicadas en el objetivo específico 1, de acuerdo Sviatun et al. (2021) en su investigación "Combating cybercrime: Economic and legal aspects" en su ponderamiento establecieron que el nivel de ciberdelincuencia en el mundo y las consecuencias económicas de su impacto tienden a aumentar. Se estima que en 2020 el costo total del cibercrimen y la ciberseguridad superará el billón de dólares estadounidenses, lo que representa más del 1 % del producto interno bruto mundial. De la misma manera, en su investigación Macías et al. (2022) "Frequent cases, criminalization and prevention of computer crimes in Ecuador" consideran, todos estos casos son relevantes en la sociedad ecuatoriana, y las leyes establecidas no han reducido los mismos, debido a que los ciberdelincuentes no tienen temor a sus acciones ilegales que realizan, debido a que sus métodos cada vez son más desarrollados y difíciles de ubicar.

Respecto al **segundo objetivo específico** se tiene en cuenta lo siguiente: Determinar el aspecto jurídico a aplicarse para tipificar las conductas delictivas del phishing para prevenir de ciberdelincuencia Lima norte 2022. Para lo cual se realizaron las siguientes preguntas:

De la **sétima pregunta** que se ha planteado en la guía de entrevista efectuada se tiene lo siguiente: En su opinión, desde la adhesión al Convenio de Budapest 2019 y la Ley n.º 30096, ¿El Perú ha podido minimizar los casos de Delitos informáticos?, para lo cual respondieron: Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Núñez (2023) y Traverso (2023), afirman que no se ha podido minimizar los casos de los delitos informáticos, debido a que los delitos informáticos evolucionan diariamente con el avance de las herramientas tecnológicas; sin embargo, no hay que menospreciar el esfuerzo que se hace en el Perú para poder minimizar la comisión de los delitos informáticos, puesto que vienen fortaleciendo las leyes y políticas en la ciberseguridad, invirtiendo en tecnología y sistemas de seguridad, además de realizar prácticas de prevención a fin de protegerse contra las amenazas cibernéticas.

De la **octava pregunta** que se ha planteado en la guía de entrevista efectuada se tiene lo siguiente: De acuerdo a su experiencia diga usted ¿Cuáles son las áreas específicas que deberían mejorarse en la Ley 30096 para abordar de manera más efectiva el incremento de la ciberdelincuencia? para lo cual respondieron: Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Núñez (2023) y Traverso (2023), afirman que para la mejora de dicha Ley se debe considerar diferentes factores, tales como el contexto legal, tecnológico y social, entre los cuales son las definiciones claras de las actividades que constituyen los delitos informáticos, además, de una adecuada pena o sanción que debe ser proporcional a la gravedad del delito, así también, se debe mejorar la cooperación internacional, puesto que muchos de los delitos informáticos son cometidos en países distintos al Perú, lo que imposibilita la obtención de mayores elementos de convicción y medios probatorios que permitan resolver la participación y comisión de estos delitos.

De la **novena pregunta** que se ha planteado en la guía de entrevista efectuada se tiene lo siguiente: En su opinión ¿Cuál sería la justificación legal más sólida para clasificar el phishing como delito y adoptar medidas preventivas contra la ciberdelincuencia?, para lo cual respondieron: Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Núñez (2023) y Traverso (2023), afirman que la justificación legal para clasificar el phishing como delito es la protección del bien jurídico, como lo es patrimonio, puesto que, al obtener la información

confidencial de las tarjetas de crédito, débito, cuentas de ahorro u otras, a través del engaño idóneo a la víctima, le causa un daño patrimonial, pues el sujeto pasivo ve mellado su patrimonio, ya que les causan daños financieros y económicos, lo que produce una desconfianza en el uso de las páginas web o el propio internet, debiendo de adoptar las medidas contra los fraudes informáticos, como la educación y concientización de los medios electrónicos a usar, la protección de datos, como las contraseñas, número de cuentas de ahorros o de tarjetas, realizar la búsqueda de información en páginas de internet seguras y que las instituciones públicas o privadas tengas políticas de seguridad y confidencialidad.

Análisis e interpretación de las categorías emergentes

De acuerdo al objetivo específico 2: Determinar el aspecto jurídico a aplicarse para tipificar las conductas delictivas del phishing para prevenir de ciberdelincuencia Lima Norte 2022.

Teniendo en cuenta el segundo objetivo específico, es importancia considerar que afirman que la justificación legal para clasificar el phishing como delito es la protección del bien jurídico, como lo es patrimonio, puesto que, al obtener la información confidencial de las tarjetas de crédito, débito, cuentas de ahorro u otras, a través del engaño idóneo a la víctima, le causa un daño patrimonial, pues el sujeto pasivo ve mellado su patrimonio.

Análisis de las fuentes documentales

Referente a las fuentes documentales indicadas en el objetivo específico 1, de acuerdo a la investigación de Ramirez et al. (2022) “Validation of a cybercrime awareness scale in Peruvian university students”, en su ponderamiento concluyeron, que los estudiantes universitarios tienen conocimiento de los modelos de cibercrimen que existen, y consideran que la sociedad debe ser capacitada ante los engaños fraudulentos de estas organizaciones dirigidas por criminales con alto conocimiento de sistemas. Igualmente, en la investigación de Vinelli (2021) “Los delitos informáticos y su relación con la criminalidad económica” , en la investigación que realizaron han identificado las actividades delictivas cometidas a través de los sistemas informáticos, que se encuentran debidamente reguladas por Ley Nº 30096, y su modificatoria Ley Nº 30171.

DISCUSIÓN

Con respecto a las discusiones que se plantean en la presente investigación, se procede al desarrollo de las mismas de acuerdo a la información obtenida de las entrevistas a los participantes expertos, que con su conocimiento enriquecen la presente investigación, para lo cual se tendrá en cuenta la información obtenida de cada uno de ellos, con respecto al objetivo general y sus específicos que se detallan a continuación:

Tabla 5

Tabla de la Discusión de Objetivo General

Objetivo General	Supuesto General
Identificar cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima Norte 2022.	Se analizó los fundamentos jurídicos para tipificar el phishing en la Ley Nº 30096 y el artículo 207-A implementado en el Perú, se enfrenta a un crecimiento del delito debido al avance de las TIC´s esto debido a su crecimiento exponencial a nivel mundial gracias al internet, este avance ha dado lugar a la ciberdelincuencia, una modalidad de acciones ilícitas que se aprovecha de la dependencia de las personas en la tecnología para realizar diversas actividades.

Nota. Elaboración propia

Para el presente análisis se tien en cuenta los criterios mencionados por los entrevistados, quienes son especialistas en el tema, para un mejor entendimiento de la materia que se está investigando.

En el **objetivo general** se tiene en cuenta a Bhavsar et al. (2018) quienes consideran que el phishing es un delito cibernético en el que se dirigen correos electrónicos, teléfonos, mensajes de texto, información de identificación personal,

como bancarios y de tarjetas de crédito y contraseñas, todo debe ser tipificado en la denuncia fiscal de acuerdo a la norma por cada país que tiene su ley respectiva.

Continuando con la conceptualización sobre el primer punto de la presente investigación, se procede a mencionar lo indicado por los entrevistados, de acuerdo a la **primera pregunta**, Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Nuñez (2023) y Traverso (2023) quienes consideraron que con el avance de la tecnología se han ido originando nuevas maneras de cometer hechos ilícitos, tal como phishing, que es una forma de fraude en línea que implica engañar a las personas, haciéndose pasar por instituciones confiables.

Es importante de acuerdo a lo señalado, que las instituciones financiera y comerciales capaciten a sus clientes, con finalidad de evitar que incurran en ingresar en páginas falsas y que su información financiera sea comprometida y tenga inconvenientes de desfalcos.

Asimismo, con respecto a la **segunda pregunta** Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Nuñez (2023) y Traverso (2023) consideraron que los elementos objetivos principales son la suplantación de identidad, el engaño o fraude, esto es, la simulación de situaciones o sucesos de hechos materiales y psicológicos, para inducir a error a su víctima, pero dicho engaño debe ser idóneo o suficiente.
Por eso es importante, que los medios electrónicos, los cuales son utilizados por ciberdelincuentes para llevar a cabo el engaño en la víctima, como por ejemplo correo electrónico, página web, mensaje de texto u otro medio.

Asimismo, respecto a la **tercera pregunta** Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Nuñez (2023) y Traverso (2023), sustentan que es muy importante poder tipificar la comisión del delito de phishing, ya que va a permitir delimitar de manera clara las acciones que van a constituir el delito en mención

Por lo tanto, se debe de considera que es importante la tipificación del phishing en cualquier sistema jurídico, con finalidad de evitar en todo momento que los

ciberdelincuentes se sigan aprovechando del robo de identidades, usando nuevas modalidades afectando a los miembros de la sociedad.

De acuerdo a lo mencionado anteriormente, considerando las opiniones de los entrevistados y de análisis efectuado, es importante mencionas las **fichas de análisis de fuente documental.** Con respecto al objetivo general, tenemos Zelada (2021) su artículo "Delitos informáticos ¿Nuevas formas de criminalidad?" donde mencionó como **texto relevante** que la ley 30096 sobre delitos informáticos busca prevenir como sancionar estas acciones ilícitas que afectan sistemas bancarios y comerciales de empresas jurídica y personas naturales. Del mismo modo, en su análisis de contenido mencionó que desde inicios del 2020 hasta la fecha, nos enfrentamos a usar nuevos aplicativos que se consideran aplicados en Ley Nº 30096 modificada por Ley Nº 30171. Del mismo modo se considera a Castañeda et al. (2021) "Vista de los delitos cibernéticos en Chile, México y Colombia", quien en su artículo manifestaron el analizar los delitos cibernéticos en los países de México, Colombia y Chile para que puedan estudiar los ordenamientos jurídicos de estas nuevas formas de delitos y ver los avances con respecto al Convenio sobre Ciberdelincuencia 2001 firmado en Budapest.

Tabla 6

Tabla de la Discusión del Objetivo Específico 1

Objetivo Específico 1	Supuesto Específico 1
Identificar cuáles son los elementos a considerarse para tipificar la conducta delictiva del phishing para prevenir la ciberdelincuencia Lima Norte 2022.	Los elementos relevantes de carácter penal tomados en cuenta para tipificar la conducta delictiva del phishing confines de prevenir la ciberdelincuencia en Lima Norte 2022 Se consideran los elementos a aquellos, a través del engaño idóneo a la víctima, le causa un daño patrimonial, pues el sujeto pasivo ve mellado su patrimonio, ya que les causan daños financieros y

	económicos, lo que produce una desconfianza en el uso de las páginas web o el propio internet, debiendo de adoptar las medidas contra los fraudes informáticos, como la educación y concientización de los medios electrónicos a usar, la protección de datos, como las contraseñas, número de cuentas de ahorros o de tarjetas, realizar la búsqueda de información en páginas de internet seguras y que las instituciones públicas o privadas tengas políticas de seguridad y confidencialidad. Por lo tanto, se cumple el supuesto del objetivo específico 1.

Nota. Elaboración propia

Asimismo, es importante considerar a los participantes (expertos), con respecto a la **cuarta pregunta** Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Nuñez (2023) y Traverso (2023), quienes concluyen, que la naturaleza jurídica del phishing, es de resultado, porque sustraen información personal de tarjetas bancarias, otras cuentas de ahorros u otra información personal y/o financiera, se configura el delito en mención.

Asimismo, es importante considerar a los participantes (expertos), con respecto a la **quinta pregunta** Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Nuñez (2023) y Traverso (2023), quienes concluyen que las modalidades principales del fraude electrónico son páginas falsas web, mediante phishing, donde las ciberdelincuencias engañan a usuarios con páginas falsas que simulan ser sitios web originales. Y en segundo término, las compras fraudulentas, que afectan cuentas de clientes de empresas comerciales que suan transacciones electrónicas.

Asimismo, es importante considerar a los participantes (expertos), con respecto a la **sexta pregunta** Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Nuñez (2023) y Traverso (2023), quienes concluyen que los últimos años a raíz de la ciberdelincuencia las transacciones virtuales bancarias se han visto afectadas por el incrementado de nuevas modalidades de delincuencia virtual, que se han desarrollado en nuevos programas fraudulentos.

De acuerdo a lo mencionado anteriormente, considerando las opiniones de los entrevistados y de análisis efectuado, es importante mencionas las **fichas de análisis de fuente documental.** Con respecto al **objetivo específico 1**, tenemos a Sviatun et al. (2021) "Combating cybercrime: Economic and legal aspects" quienes consideraron en su investigación que el cibercrimen amenaza la seguridad nacional de diferentes países del mundo. El crecimiento de los ciberataques desestabiliza el orden internacional y trastorna el normal funcionamiento de las relaciones internacionales. Asimismo, Macías et al. (2022) "Frequent cases, criminalization and prevention of computer crimes in Ecuador", determinaron en su investigación, que los delitos informáticos a nivel mundial y en el Ecuador se han incrementado en forma exponencial a partir del año 2020, debido especialmente a suplantar personas, falsificar documentos, entre otra información confidencias de los usuarios de sistemas virtuales.

Tabla 7

Tabla de discusión del Objetivo Específico 2

Objetivo Específico 2	Supuesto Específico 2
Determinar el aspecto jurídico a aplicarse para tipificar conductas delictivas del phishing para prevenir de ciberdelincuencia Lima norte 2022.	La naturaleza jurídica que se debe considerar para tipificar la conducta delictiva del phishing como prevención de ciberdelincuencia Lima Norte 2022. Se le considera que son delitos de resultado, por lo tanto, debe se considerarse como una acción que, del provecho injusto sobre el patrimonio de un agraviado, lo cual es considerado

	delito quedando que no podría dejarse de lado en forma tentativa.

Nota. Elaboración propia

Asimismo, es importante considerar a los participantes (expertos), con respecto a la **sétima pregunta** Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Nuñez (2023) y Traverso (2023), quienes concluyen, que no existe posibilidad de disminuir casos de los delitos informáticos, debido a que los delitos informáticos evolucionan diariamente con el avance de las herramientas tecnológicas; sin embargo, no hay que menospreciar el esfuerzo que se hace en el Perú para poder minimizar estos delitos.

Asimismo, es importante considerar a los participantes (expertos), con respecto a la **octava pregunta** Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Nuñez (2023) y Traverso (2023), quienes concluyen, que para la mejora de dicha Ley se debe considerar diferentes factores, tales como el contexto legal, tecnológico y social, entre los cuales son las definiciones claras de las actividades que constituyen los delitos informáticos

Asimismo, es importante considerar a los participantes (expertos), con respecto a la **novena pregunta** Mendoza (2023), Cajo (2023), Méndez (2023), Cari (2023), Soto (2023), Nuñez (2023) y Traverso (2023), quienes concluyen, que la justificación legal para clasificar el phishing como delito es la protección del bien jurídico, como lo es patrimonio, puesto que, al obtener la información confidencial de las tarjetas de crédito, débito, cuentas de ahorro u otras, a través del engaño idóneo a la víctima, le causa un daño patrimonial, pues el sujeto pasivo ve mellado su patrimonio.

De acuerdo a lo mencionado anteriormente, considerando las opiniones de los entrevistados y de análisis efectuado, es importante mencionas las **fichas de análisis de fuente documental.** Con respecto al **objetivo específico 2**, se ha considerado a Ramirez et al. (2022) “Validation of a cybercrime awareness scale in Peruvian university students”, quienes en su investigación que realizaron fue determinar como la conciencia en estudiantes universitarios, sobre la identificación de los principales indicadores sobre los cibercrímenes en nuestra sociedad y

enumerarlos de acuerdo a su importancia. Del mismo modo, Vinelli (2021) Los delitos informáticos y su relación con la criminalidad económica", en la investigación que realizaron han identificado las actividades delictivas cometidas a través de los sistemas informáticos, que se encuentran debidamente reguladas por Ley Nº 30096, y su modificatoria Ley Nº 30171.

V. CONCLUSIONES

PRIMERA: La tipificación del phishing a pesar que existen leyes que la sancionan como la Ley 30096 y Ley 30171 (que la modifica) no son todos sancionados, debido a que con el avance de la tecnología se han ido originando nuevas maneras de cometer hechos ilícitos, tal como Smishing, Vishing, entre otros, se van incrementando en diversas formas de fraude en línea que implica engañar autoridades o clientes, haciéndose pasar por instituciones legítimas, con finalidad de adquirir datos confidenciales de tarjetas de crédito, tal como las contraseñas, números de tarjetas y demás detalles, siendo que dichos actos ocasionan daños financieros y personales a las víctimas, lo que ocasiona que las personas pierdan la confianza en las transacciones que se hacen a través del internet. Por lo tanto se recomienda, que se debe de mejorar el artículo 207-A.

SEGUNDA: Debido a que ante la ausencia de un tipo penal detallado del phishing, es necesario que la investigaciones de las fiscalías, por eso en la carpeta fiscal como instrumento técnico de elaboración de la documentación sobre los requerimientos de acusación, se debe de mencionar que esta acción delictiva del phishing debe ser tipificada como delitos contra el patrimonio bajo la modalidad de estafa simple o agravada, considerando a los elementos típicos del phishing detallados en la investigación.

TERCERA: Con respecto a la naturaleza jurídica o delictiva del phishing que se debe de adoptar, se debe tener en cuenta que en primera instancia se deben de concebir como delitos de peligro cuyo bien jurídico es proteger la seguridad informática y en segunda instancia, cuando los delitos de los ciberdelincuentes agravan la naturaleza jurídica, debe el fiscal cambiar la naturaleza jurídica a delitos de resultados para poder proteger al usuario.

VI. RECOMENDACIONES

PRIMERA: Se recomienda a congresistas que deben regular las nuevas modalidades de delitos informáticos como tipo penales detallados, de acuerdo conducta delictiva denominada phishing en la Ley Nº 30096 y su modificación en la Ley Nº 30171.

SEGUNDA: Del mismo modo, recomendar Fiscal de la Nación y miembros del poder judicial, ejercer sus acciones sobre nuevas acciones del delito informático, como Phishing y otros, como una conducta específica en la Ley Nº 30096.

TERCERA: Se recomienda al Gobierno Central incrementar el presupuesto asignando a la Policía Nacional del Perú y Ministerio Público, para enfrentar con mejor eficiencia y eficacia contra los delitos informáticos, que se siguen incrementando a nivel nacional.

REFERENCIAS

Acosta, M., Benavides, M., & García, N. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, 25*(89), 1-12. https://www.redalyc.org/journal/290/29062641023/html/

Alcalá, M., & Meléndez, M. (2023). Delitos informáticos en México. Reconocimiento en los ordenamientos penales de las entidades mexicanas. *Paakat: Revista de Tecnología y Sociedad, 13*(24), 1-37. http://www.udgvirtual.udg.mx/paakat/index.php/paakat/article/view/759/pdf

Baena, G. (2017). *Metodología de la investigación.* México: Grupo Editorial Patria. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/metodologia%20de%20la%20investigacion.pdf

Benavides, E., & Fuertes, W. S. (2020). Caracterización de los ataques de phishing y técnicas para mitigarlos. Ataques: una revisión sistemática de la literatura. *Ciencia y Tecnología, 13*(1), 97-104. https://dialnet.unirioja.es/descarga/articulo/7563018.pdf

Bhavsar, V., Kadlak, A., & Sharma, S. (2018). Study on Phishing Attacks . *International Journal of Computer Applications, 182*(33), 27-29. https://www.researchgate.net/publication/329716781_Study_on_Phishing_Attacks

Cabezas, E., Andrade, D., & Torres, J. (2018). *Introducción a la Metodología de la Investigación Científica.* Universidad de las Fuerzas Armadas ESPE. http://repositorio.espe.edu.ec/xmlui/handle/21000/15424

Calvo, M. (2022). The civil liability og Banks in the crimes of fraud by Phishing. *Actualidad Jurídica Iberoamericana*(18), 1788-1809. https://revista-aji.com/articulos/2023/18/AJI18_64.pdf

Cámara, S. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social*(60), 470-512. https://dialnet.unirioja.es/descarga/articulo/7524987.pdf

Cámara, S. (2020). Estudios criminológicos contemporáneos (IX): La Cibercriminología y el perfil del ciberdelincuente. *Derecho y Cambio Social*(60), 1-43. https://dialnet.unirioja.es/descarga/articulo/7524987.pdf

Castañeda, R., Flores, H., & Castro, E. (2021). Vista de los delitos cibernéticos en Chile, México y Colombia". *Ius Comitiãlis, 4*(8), 252-276. https://iuscomitialis.uaemex.mx/article/view/17320/12891

Congreso. (21 de Octubre de 2013). *Congreso de la Republica*. Congreso de la Republica: https://www2.congreso.gob.pe/sicr/cendocbib/con5_uibd.nsf/C5F98BB564E5CCCF05258316006064AB/$FILE/6_Ley_30096.pdf

De La Torre, C., & Quiroz, J. (2023). Ciberdelito y su asociación en el cometimiento de fraudes financieros en la pandemia de la COVID-19. *Revista Venezolana de Gerencia, 28*(102), 609-628. doi:https://doi.org/10.52080/rvgluz.28.102.11

Devanny, J., Luiz, F., & Medeiros, B. (2022). The rise of cyber power in Brazil. *Revista Brasileira de Política Internacional, 65*(1), 3-22. https://www.redalyc.org/journal/358/35870295010/35870295010.pdf

Durán, M. (2018). Uso de lista de cotejo. *Universidad Tecnológica Metropolitana*, 1-21. https://vrac.utem.cl/wp-content/uploads/2018/10/manua.Lista_Cotejo-1.pdf

Erazo, M. (2018). Rigor científico en las prácticas de investigación cualitativa. *Ciencia, Docencia y Tecnología, 22*(42), 107-136. https://www.researchgate.net/publication/262668263_Rigor_cientifico_en_las_practicas_de_investigacion_cualitativa

Feria, H., Mantilla, M., & Mantecón, S. (2019). La triangulación metodológica como método de la investigación científica. Apuntes para una conceptualización. *Didáctica y Educación, 10*(4), 136-146. https://revistas.ult.edu.cu/index.php/didascalia/article/view/917

Flores, C., Rodríguez, T., Urbizagastegui, J., Guerra, L., & Retuerto, L. (2022). *Ciberdelincuencia: Reporte de información estadistica y recomendaciones para la prevención.* Lima: Observatorio Nacional de Política Criminal. https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf

Hernández, A., & Baluja, a. (2021). Principales mecanismos para el enfrentamiento al phishing en las redes de datos . *Revista Cubana de Ciencias Informáticas, 15*, 413-441. https://www.redalyc.org/journal/3783/378370462024/html/

Hernandez, R., Fernández, C., & Baptista, M. (2017). *Metodología de la Investigación.* México DF, México: McGraw-Hilli / Interamericana Editores, S.A. de C.V.

Jiménez, R. (2021). *Proyecto Robo de Datos y Fraude a través de Canales Digitales.* Honduras: Unidad de Inteligencia Financiera. https://pplaft.cnbs.gob.hn/wp-content/uploads/2021/04/Informe-de-proyecto-Robo-de-datos-y-Fraude-a-traves-de-Canales-Digitales.pdf

La Madriz, J. (2019). *Metodología de la Investigación: Actuación humana orientada al conocimiento.* Guayaquil: CIDE Editorial. http://repositorio.cidecuador.org/bitstream/123456789/75/1/Metodologia%20de%20la%20Investigacion.pdf

Leya, C. (2021). Estudio de los delitos informáticos y la problemática de su tipificación en el marco de los convenios internacionales. *Lucerna Iuris Et Investigatio*(1), 29-47. https://revistasinvestigacion.unmsm.edu.pe/index.php/Lucerna/article/download/18373/16528/68634

Macías, R., Boné, M., Quiñonez, F., Mendoza, J., Estupiñan, G., & Rodríguez, J. (2022). Frequent cases, criminalization and prevention of computer crimes in Ecuador: a brief systematic review. *Sapienza: International Journal of Interdisciplinary Studies, 3*(2), 231-243. https://journals.sapienzaeditorial.com/index.php/SIJIS/article/view/324

Nuñez, F., & Carhuancho, B. (2020). Ciberdelincuencia en tiempos de Covid-19: ¿La vulneración a derechos constitucionales? *Lumen, 16*(1), 93-100. https://revistas.unife.edu.pe/index.php/lumen/article/download/2287/2359/7097

Ortiz, N. (2019). Normativa Legal sobre Delitos Informáticos en Ecuador. *Revista Científica Hallazgos 21, 4*(1), 100-111. https://www.academia.edu/43061757/Delitos_Informaticos

Parada, R., & Errecaborde, J. (2018). *Cibercrimen y delitos informáticos : los nuevos tipos penales en la era de internet.* Buenos Aires: Revista ERREIUS. https://www.pensamientopenal.com.ar/system/files/2018/09/doctrina46963.pdf

Patayo, C. (2021). A Preventive and Detective Model for Phishing Attack in Small

and Medium Size Businesses. *Journal of Bugema University*, 1-16. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3777065

Peña, T. (2022). Etapas del análisis de la información documental. *Revista Interamericana de Bibliotecología, 45*(3), 1-7. http://www.scielo.org.co/pdf/rib/v45n3/2538-9866-rib-45-03-e4.pdf

Peruano, E. (04 de 09 de 2022). Denuncias por delitos informáticos se incrementaron en más del 90% en el Perú. *Diario El Peruano*, págs. 1-2. https://www.elperuano.pe/noticia/188048-denuncias-por-delitos-informaticos-se-incrementaron-en-mas-del-90-en-el-peru

Pichihua, S. (16 de Enero de 2020). Estos son los delitos informáticos más frecuentes en el Perú, según la Policía. *Agencia Andina*, pág. 1. https://andina.pe/agencia/noticia-estos-son-los-delitos-informaticos-mas-frecuentes-el-peru-segun-policia-781320.aspx

Piña, H. (2019). Cibercriminalidad y ciberseguridad en México. *Ius Comitiãlis, 2*(4), 47-69. https://iuscomitialis.uaemex.mx/article/view/13203/10538

Quintana, L., & Hermida, J. (2019). La hermenéutica como método de interpretación de textos en la investigación psicoanalítica. *Revista de Psicología y Ciencias Afines, 16*(2), 73-80. https://www.redalyc.org/journal/4835/483568603007/html/

Ramírez, E., Toledo, R., Norabuena, R., & Henostroza, P. (2022). Validation of a cybercrime awareness scale in Peruvian university students. *Revista Científica General José María Córdova, 20*(37), 209-224. http://www.scielo.org.co/pdf/recig/v20n37/2500-7645-recig-20-37-208.pdf

Riega, Y., Huamani, H., & Machuca, J. (2021). Contratación electrónica y los delitos informáticos. En protección al consumidor en el Perú. *Revista Lex, 19*(28), 199-236. http://revistas.uap.edu.pe/ojs/index.php/LEX/article/view/2318

Salvador, W. (2022). Derecho a la intimidad y la ciberdelincuencia. Efectos sociales y económicosenvíctimas ecuatorianas. *Revista Mundo Financiero, 3*(9), 41-55. https://mundofinanciero.indecsar.org/revista/index.php/munfin/article/view/74/79

Sánchez, H., Reyes, C., & Mejía, S. (2018). *Manual de términos en investigación científica, tecnologíca y humanística.* Lima: Universidad Ricardo Palma.

https://www.urp.edu.pe/pdf/id/13350/n/libro-manual-de-terminos-en-investigacion.pdf

Santos, A., & Texeira, R. (2020). *Delitos Cibernéticos: Nociones Básicas.* Santa Catalina: Revista Universidada Federal de Santa Catalina. https://www.casede.org/index.php/biblioteca-casede-2-0/seguridad/ciberseguridad/672-delitos-ciberneticos-nociones-basicas/file

Sviatun, O., Goncharuk, O., Roman, C., Kuzmenko, O., & Kozych, I. (2021). Combating cybercrime: economic and legal aspects. *Wseas transactions on enirоment and , 17*, 542-552. https://www.researchgate.net/publication/351740010_Combating_Cybercrime_Economic_and_Legal_Aspects

Vinelli, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. *Ius et Praxis, Revista de la Facultad de Derecho*(53), 95-110. https://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/download/4995/5428/

Zelada, E. (2021). Delitos informáticos ¿Nuevas formas de criminalidad? *Revista deleyes*, 1-3. https://www.deleyes.pe/articulos/delitos-informaticos-nuevas-formas-de-criminalidad

ANEXOS

Anexo 1. Matriz de categorización

CATEGORÍAS	DEFINICIÓN CONCEPTUAL	SUBCATEGORÍAS	CÓDIGO	PROBLEMAS GENERAL	OBJETIVOS GENERAL	SUPUESTOS	METODOLOGÍA
Tipificación del phishing en el sistema penal peruano Prevención de la ciberdelincuencia	En el Perú se aprobó la Ley 30096 (2013) denominada ley de delitos informáticos y modifica en algunos artículos en la ley 30171 publicada en marzo del 2014, la cual se encuentra relacionada sobre Convenio sobre la Ciberdelincuencia de Budapest del año 2001. Benavides et al. (2020) el phishing es conocido como una combinación de ingeniera y exploits técnicos, a través de los cuales convencen a las personas en proporcionar sus claves o datos personales para acceder a sus diversas cuentas personales en entidades bancarias, financieras y comerciales.	• Ley No. 30096 - Delitos informáticos. • Proceso judicial: casos de ciberdelincuencia. • Administración de Justicia. • División de Investigación de delitos de Alta Tecnología.		**Problema general** ¿Cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima norte 2022? **Problema específico** ¿Cuáles serían aquellos elementos que se deben de tener en cuenta para tipificar la conducta delictiva del phishing para la prevención de ciberdelincuencia Lima norte 2022? ¿Cuál sería la naturaleza jurídica que se debe considerar para tipificar la conducta delictiva del phishing como prevención de ciberdelincuencia Lima norte 2022?	**Objetivos generales** Identificar los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia. **Objetivos específicos** Identificar los elementos que se deben de tener en cuenta para tipificar la conducta delictiva del phishing para la prevención de ciberdelincuencia Lima norte 2022. ¿Determinar la naturaleza jurídica que se debe considerar para tipificar la conducta delictiva del phishing como prevención de ciberdelincuencia Lima norte 2022?	**Supuesto General**, los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia, por otro lado, el **Supuesto Específico 1** Elementos a considerarse para tipificar la conducta delictiva del phishing para prevenir la ciberdelincuencia en Lima Norte 2022 **Supuesto Específico 2**, Naturaleza jurídica que se debe considerar para tipificar la conducta delictiva del phishing como prevención de ciberdelincuencia Lima Norte 2022.	Enfoque cualitativo Diseño de investigación Fenomenológico Tipo de Investigación Básica Nivel de Investigación Descriptiva Escenario de estudio Ministerio publico Participantes Fiscales Asistente en función Fiscal y Asistente Administrativo TÉCNICA E INSTRUMENTO DE RECOLECCION DE DATOS Entrevista – Guía de entrevista.

Nota no se han utilizado códigos ni abreviaturas
Elaboración propia

Anexo 2

GUÍA DE ENTREVISTA

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

TÍTULO

"La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima norte 2022"

ENTREVISTADO/A :

CARGO :

FECHA :

Las tecnologías de la información (TIC) han experimentado un crecimiento exponencial a nivel mundial gracias al internet. Esto ha facilitado la administración, procesamiento y compartición de información a través de diferentes dispositivos como computadoras, laptops, teléfonos móviles y televisores. Sin embargo, este avance ha dado lugar a la ciberdelincuencia, una modalidad de acciones ilícitas que se aprovecha de la dependencia de las personas en la tecnología para realizar diversas actividades.

El presente instrumento pretende recopilar su opinión respecto a este tema, en el cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales

Objetivo General

Identificar cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 1: A su criterio ¿Considera usted que los delitos del phishing deben ser incorporados y penalizados en nuestro sistema de justicia?

Pregunta 2: A su criterio ¿Cuáles serían los elementos objetivos que deben ser considerados a fin de tipificar dichas conductas?

Pregunta 3: En su opinión ¿Considera que es importante la tipificación de las modalidades como el Phishing, en nuestro ordenamiento jurídico?

OBJETIVO ESPECÍFICO 1

Identificar cuáles son los elementos a considerarse para tipificar la conducta delictiva del phishing para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 4: En base a su experiencia ¿Qué naturaleza jurídica debe adoptar la tipificación de las conductivas del Phishing, de resultado o peligro?

Pregunta 5: En base a su experiencia diga usted ¿Cuáles son las modalidades más frecuentes en el Perú, para la comisión del delito de fraude informático?

Pregunta 6: A su criterio ¿La ciberdelincuencia se incrementa debido a falta de una ley adecuada?

OBJETIVO ESPECÍFICO 2

Determinar el aspecto jurídico a aplicarse para tipificar las conductas delictivas del phishing para prevenir de ciberdelincuencia Lima norte 2022.

Pregunta 7: En su opinión, desde la adhesión al Convenio de Budapest 2019 y la Ley n.º 30096, ¿El Perú ha podido minimizar los casos de Delitos informáticos?

Pregunta 8: De acuerdo a su experiencia diga usted ¿Cuáles son las áreas específicas que deberían mejorarse en la Ley 30096 para abordar de manera más efectiva el incremento de la ciberdelincuencia?

Pregunta 9: En su opinión ¿Cuál sería la justificación legal más sólida para clasificar el phishing como delito y adoptar medidas preventivas contra la ciberdelincuencia?

FIRMA Y SELLO

Anexo 3 - Entrevista # 1

GUÍA DE ENTREVISTA

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

TÍTULO

"La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima norte 2022"

ENTREVISTADO/A : JUAN MANUEL MENDEZ NAVARRO

CARGO : FISCAL PROVINCIAL PENAL LIMA NORTE

FECHA : 27 DE OCTUBRE DEL 2023

Las tecnologías de la información (TIC) han experimentado un crecimiento exponencial a nivel mundial gracias al internet. Esto ha facilitado la administración, procesamiento y compartición de información a través de diferentes dispositivos como computadoras, laptops, teléfonos móviles y televisores. Sin embargo, este avance ha dado lugar a la ciberdelincuencia, una modalidad de acciones ilícitas que se aprovecha de la dependencia de las personas en la tecnología para realizar diversas actividades.

El presente instrumento pretende recopilar su opinión respecto a este tema, en el cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales

Objetivo General

Identificar cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 1: A su criterio ¿Considera usted que los delitos del phishing deben ser incorporados y penalizados en nuestro sistema de justicia?

De acuerdo, deben ser tomados en cuenta en el sistema jurídico, porque artículo 207-A ha sido normado muy genérico según modalidades actuales de delincuencia virtual porque se han innovado en este aspecto.

Pregunta 2: A su criterio ¿Cuáles serían los elementos objetivos que deben ser considerados a fin de tipificar dichas conductas?
Se debe de considerar de acuerdo como se lleva a delante la lesión al bien jurídico, en el actuar doloso y según medios para dicho fin.

Pregunta 3: En su opinión ¿Considera que es importante la tipificación de las modalidades como el Phishing, en nuestro ordenamiento jurídico?

Exacto, estas deben ser tipificadas de forma detallada y específica, debido que la tipificación se considera ambigua en el Articulo 207-A del código penal.

OBJETIVO ESPECÍFICO 1

Identificar cuáles son los elementos a considerarse para tipificar la conducta delictiva del phishing para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 4: En base a su experiencia ¿Qué naturaleza jurídica debe adoptar la tipificación de las conductivas del Phishing, de resultado o peligro?

Son considerados como delitos de resultados, porque debe de tener en cuenta su materialización la acción de aprovecharse del patrimonio de una persona agraviada al considerarse este delito, además tener en cuenta la ejecución del hecho.

Pregunta 5: En base a su experiencia diga usted ¿Cuáles son las modalidades más frecuentes en el Perú, para la comisión del delito de fraude informático?

Realmente en la actualidad la delincuencia usando el fraude informático, es hacerse pasar en la web por cualquier institución bancaria, con finalidad de poder acceder a sus contraseñas y cometer el delito de fraude.

Pregunta 6: A su criterio ¿La ciberdelincuencia se incrementa debido a falta de una ley adecuada?

Exactamente, los últimos años la ciberdelincuencia se ha incrementado debido a la masificación de los medios informáticos por incremento de nuevas tecnologías en telecomunicaciones.

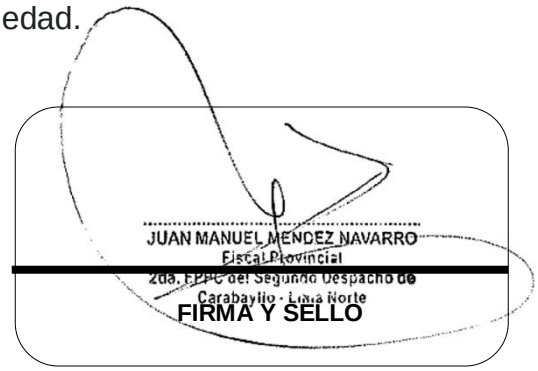
OBJETIVO ESPECIFICO 2

Determinar el aspecto jurídico a aplicarse para tipificar las conductas delictivas del phishing para prevenir de ciberdelincuencia Lima norte 2022.

Pregunta 7: En su opinión, desde la adhesión al Convenio de Budapest 2019 y la Ley n.º 30096, ¿El Perú ha podido minimizar los casos de Delitos informáticos?
Caso contrario, debido que la unidad responsable de lucha contra el la ciberdelincuencia no tiene los recursos suficientes para luchar con este tipo de delincuencia virtual.

Pregunta 8: De acuerdo a su experiencia diga usted ¿Cuáles son las áreas específicas que deberían mejorarse en la Ley 30096 para abordar de manera más efectiva el incremento de la ciberdelincuencia?
Debe de incrementarse recursos tanto de personal como financieros para que la Policía Nacional del Perú (PNP) y el Ministerio Público (MP) puedan combatir este flagelo social.

Pregunta 9: En su opinión ¿Cuál sería la justificación legal más sólida para clasificar el phishing como delito y adoptar medidas preventivas contra la ciberdelincuencia?
La principal causa que afectan estos delincuentes es la afectación del patrimonio de los ciudadanos y afecta la paz social en la sociedad.



FIRMA Y SELLO

Anexo 4 – Entrevista # 2

GUÍA DE ENTREVISTA

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

TÍTULO

“La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima norte 2022”

ENTREVISTADO/A : VICTOR ALBERTO MENDOZA ROBLES

CARGO :FISCAL PROVINCIAL LIMA NORTE

FECHA : 27 DE OCTUBRE DEL 2023

Las tecnologías de la información (TIC) han experimentado un crecimiento exponencial a nivel mundial gracias al internet. Esto ha facilitado la administración, procesamiento y compartición de información a través de diferentes dispositivos como computadoras, laptops, teléfonos móviles y televisores. Sin embargo, este avance ha dado lugar a la ciberdelincuencia, una modalidad de acciones ilícitas que se aprovecha de la dependencia de las personas en la tecnología para realizar diversas actividades.

El presente instrumento pretende recopilar su opinión respecto a este tema, en el cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales

Objetivo General

Identificar cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 1: A su criterio ¿Considera usted que los delitos del phishing deben ser incorporados y penalizados en nuestro sistema de justicia?

Ante la ocurrencia, generalización y evolución de este tipo de delitos en perjuicio de los ciudadanos, resultaría necesario la penalización, como un mecanismo de prevención general. Incorporando los delitos de phishing , como las de pharming y carding con los que reducirán el índice de ciberdelincuencia en nuestro país.

Pregunta 2: A su criterio ¿Cuáles serían los elementos objetivos que deben ser considerados a fin de tipificar dichas conductas?

Que, los elementos objetivos palmarios serian que mediante medios informáticos **suplanta la identidad de una persona** con el objeto de engañar, valiéndose de la **confianza** que esta tiene en las organizaciones para revelar información confidencial, agregándose la vulneración de esta información sensible, presupuestos y/o elementos que sumarian para tipificar el delito en cuestión.

Pregunta 3: En su opinión ¿Considera que es importante la tipificación de las modalidades como el Phishing, en nuestro ordenamiento jurídico?

Conforme se señalo siendo muy recurrente estas conductas resulta importante la regulación de esta acción dolosa, para su ulterior reproche penal.

OBJETIVO ESPECIFICO 1

Identificar cuáles son los elementos a considerarse para tipificar la conducta delictiva del phishing para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 4: En base a su experiencia ¿Qué naturaleza jurídica debe adoptar la tipificación de las conductivas del Phishing, de resultado o peligro?

En atención a la modalidad delictiva la naturaleza de este tipo penal debería ser de mero peligro, no siendo exigible el resultado.

Pregunta 5: En base a su experiencia diga usted ¿Cuáles son las modalidades más frecuentes en el Perú, para la comisión del delito de fraude informático?

Las modalidades serian en primer término, las lágrimas clonadas falsas, a través del phishing, donde las ciberdelincuencias engañan a los usuarios con paginas falsas que simulan ser los sitios web de los bancos o entidades financieras. En segundo; termino, las compras fraudulentas, donde los bancos o entidades financieras. En segundo; termino, las compras fraudulentas, donde los ciberdelincuentes ofertan productos online, donde se falsifican ofertas o descuentos de reconocidas tiendas en línea, acción que lesiona cada vez mas frecuentes a través de mensajes de texto o notificaciones donde se acceden a sitios web clonados.

Pregunta 6: A su criterio ¿La ciberdelincuencia se incrementa debido a falta de una ley adecuada?

En primer término, por la falta de diligencia de los usuarios de plataformas web, y segundo, por la ausencia de información de las redes involucradas en estas actividades que deberían tener plataformas de web mas seguros y difundir las modalidades usadas por los ciberlincuentes. Luego es la necesidad de una regulación preventiva y ulteriormente y una regulación punitiva como exige la población.

OBJETIVO ESPECIFICO 2

Determinar el aspecto jurídico a aplicarse para tipificar las conductas delictivas del phishing para prevenir de ciberdelincuencia Lima norte 2022.

Pregunta 7: En su opinión, desde la adhesión al Convenio de Budapest 2019 y la Ley n.º 30096, ¿El Perú ha podido minimizar los casos de Delitos informáticos?

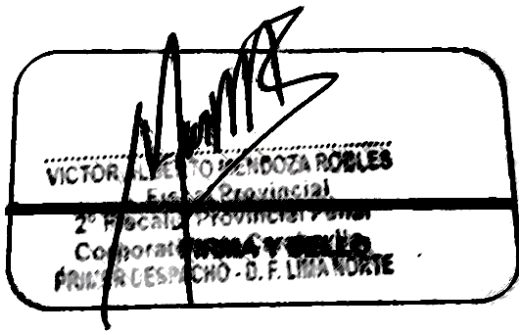
En mi opinión cualquier instrumento jurídico que permite a los operadores de justicia realizar sus labores, es notable, en la medida que estén acompañadas de otros instrumentos de prevención y que estos estén difundidos razonablemente, dentro de un político criminal no coyunturas y de ser el caso responsable, estos son, comprometido en la lucha frontal contra estos actos.

Pregunta 8: De acuerdo a su experiencia diga usted ¿Cuáles son las áreas específicas que deberían mejorarse en la Ley 30096 para abordar de manera más efectiva el incremento de la ciberdelincuencia?

En la actualidad y, debido al incremento del uso de las redes informática y la información electrónica para cometer delitos, resulta urgente y necesario contar con herramientas eficaces para la lucha con esta nueva forma de criminalidad, abonándose con el apoyo cooperaciones judicial internacionales, con el compromiso de todos los actores involucrados en el tema.

Pregunta 9: En su opinión ¿Cuál sería la justificación legal más sólida para clasificar el phishing como delito y adoptar medidas preventivas contra la ciberdelincuencia?

El perjuicio muy recurrente, abonado a la sensación de impunidad en los justiciables, por no alcanzar el reproche en los casos que se avocan, ello se suma a la falta de regulación clara donde se describa el tipo penal y la sanción ejemplar.



Anexo 5 – Entrevista # 3

GUÍA DE ENTREVISTA

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

TÍTULO

"La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima norte 2022"

ENTREVISTADO/A : ALEXANDER TRAVERZO WISSAR

CARGO : FISCAL ADJUNTO PROVINCIAL PENAL DE LIMA NORTE

FECHA : 27 OCTUBRE DEL 2023

Objetivo General

Identificar cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima norte 2022

Las tecnologías de la información (TIC) han experimentado un crecimiento exponencial a nivel mundial gracias al internet. Esto ha facilitado la administración, procesamiento y compartición de información a través de diferentes dispositivos como computadoras, laptops, teléfonos móviles y televisores.

El presente instrumento pretende recopilar su opinión respecto a este tema, en el cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales.

Pregunta 1: A su criterio ¿Considera usted que los delitos del phishing deben ser incorporados y penalizados en nuestro sistema de justicia?

Si, deben ser ingresados como tal a nuestro sistema jurídico, ya que el articulo 207-A es muy genérico respecto de las modalidades y de las formas en las que se Lleva adelante este actuar criminal.

Pregunta 2: A su criterio ¿Cuáles serían los elementos objetivos que deben ser considerados a fin de tipificar dichas conductas?
Los sujetos activo y pasivo, el modo en el que se lleva adelante la lesión al bien jurídico y a la norma penal como resultado del actuar doloso y los medios comisivos para dicho fin

Pregunta 3: En su opinión ¿Considera que es importante la tipificación de las modalidades como el Phishing, en nuestro ordenamiento jurídico?

Deben ser tipificadas de forma específica, ya que, como mencionamos anteriormente, solo se ha hecho una tipificación muy ambigua en el Articulo 207-A del código penal.

OBJETIVO ESPECIFICO 1
Identificar cuáles son los elementos a considerarse para tipificar la conducta delictiva del phishing para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 4: En base a su experiencia ¿Qué naturaleza jurídica debe adoptar la tipificación de las conductivas del Phishing, de resultado o peligro?

Son delitos de resultado, por cuanto debe materializarse la acción del provecho injusto sobre el patrimonio del agraviado para que pueda considerarse delito, por otro lado no podrá dejarse de lado la tentativa como posición en la ejecución del hecho, por cuanto es la manifestación de voluntad antijuridica que se ve truncada por situaciones externas o internas que Ilustran el resultado final.

Pregunta 5: En base a su experiencia diga usted ¿Cuáles son las modalidades más frecuentes en el Perú, para la comisión del delito de fraude informático?

La modalidad mas frecuente es hacerse pasar por una empresa en la web para poder secuestrar los datos sensibles y luego poder acceder a las claves o contraseñas.

Pregunta 6: A su criterio ¿La ciberdelincuencia se incrementa debido a falta de una ley adecuada?

Ha ido aumentando en los últimos años por la masificación de los medios de comunicación y el aumento de las tecnologías en telecomunicaciones

OBJETIVO ESPECIFICO 2

Determinar el aspecto jurídico a aplicarse para tipificar las conductas delictivas del phishing para prevenir de ciberdelincuencia Lima norte 2022.

***-Pregunta 7:** En su opinión, desde la adhesión al Convenio de Budapest 2019 y la Ley N.º 30096, ¿El Perú ha podido minimizar los casos de Delitos informáticos?

En lo absoluto, si bien es cierto se ha generado una unidad específica de lucha contra la delincuencia. esta resulta manifiestamente insuficiente por falta de protocolos de protección y de encriptación de las contraseñas, su obtención fraudulenta y su posterior uso en el mercado negro.

Pregunta 8: De acuerdo a su experiencia diga usted ¿Cuáles son las áreas específicas que deberían mejorarse en la Ley 30096 para abordar de manera más efectiva el incremento de la ciberdelincuencia?

Un aumento en los recursos que utiliza la Policía Nacional del Perú y el Ministerio Público para lograr combatir este flagelo social.

Pregunta 9: En su opinión ¿Cuál sería la justificación legal más sólida para clasificar el phishing como delito y adoptar medidas preventivas contra la ciberdelincuencia?

La principal causa seria que causa lesión al patrimonio de la ciudadanía y que no permite mantener la paz social dentro de la convivencia social

FIRMA Y SELLO

Anexo 6 – Entrevista # 4

GUÍA DE ENTREVISTA

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

TÍTULO

“La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima norte 2022”

ENTREVISTADO/A : DEYDA SOTO ROJAS

CARGO : FISCAL ADJUNTA LIMA NORTE

FECHA : 27 DE OCTUBRE DEL 2023

Las tecnologías de la información (TIC) han experimentado un crecimiento exponencial a nivel mundial gracias al internet. Esto ha facilitado la administración, procesamiento y compartición de información a través de diferentes dispositivos como computadoras, laptops, teléfonos móviles y televisores. Sin embargo, este avance ha dado lugar a la ciberdelincuencia, una modalidad de acciones ilícitas que se aprovecha de la dependencia de las personas en la tecnología para realizar diversas actividades.

El presente instrumento pretende recopilar su opinión respecto a este tema, en el cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales

Objetivo General

Identificar cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 1: A su criterio ¿Considera usted que los delitos del phishing deben ser incorporados y penalizados en nuestro sistema de justicia?

Si es correcto, incorporados a nuestro sistema jurídico, teniendo en cuenta que el artículo 207-A no es muy detallado al respecto a las diversas modalidades como actúan los criminales virtuales.

Pregunta 2: A su criterio ¿Cuáles serían los elementos objetivos que deben ser considerados a fin de tipificar dichas conductas?
Se debe de considerar a los sujetos que son activo y pasivo, de acuerdo al modo como se conde la lesión al bien jurídico y norma penal según el actuar doloso.

Pregunta 3: En su opinión ¿Considera que es importante la tipificación de las modalidades como el Phishing, en nuestro ordenamiento jurídico?

De acuerdo, deben ser tipificadas en forma detallada y específico, teniendo en cuenta que el artículo 207-A es muy genérico.

OBJETIVO ESPECIFICO 1
Identificar cuáles son los elementos a considerarse para tipificar la conducta delictiva del phishing para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 4: En base a su experiencia ¿Qué naturaleza jurídica debe adoptar la tipificación de las conductivas del Phishing, de resultado o peligro?

Se le considera que son delitos de resultado, por lo tanto, debe se considerarse como una acción que del provecho injusto sobre el patrimonio de un agraviado, lo cual es considerado delito quedando que no podría dejarse de lado en forma tentativa.

Pregunta 5: En base a su experiencia diga usted ¿ Cuáles son las modalidades más frecuentes en el Perú, para la comisión del delito de fraude informático?

La modalidad considerada más frecuentes es cuando sorprenden a usuarios de entidades financieras en páginas web, para acceder

Pregunta 6: A su criterio ¿La ciberdelincuencia se incrementa debido a falta de una ley adecuada?

Es correcta su apreciación, además los últimos a raíz de la delincuencia las transacciones virtuales bancarias se han incrementado y los ciberdelincuentes se han desarrollado en nuevos programas fraudulentos.

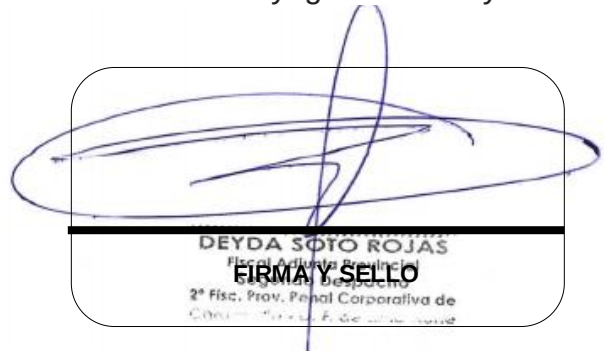
OBJETIVO ESPECIFICO 2

Determinar el aspecto jurídico a aplicarse para tipificar las conductas delictivas del phishing para prevenir de ciberdelincuencia Lima norte 2022.

Pregunta 7: En su opinión, desde la adhesión al Convenio de Budapest 2019 y la Ley n.º 30096, ¿El Perú ha podido minimizar los casos de Delitos informáticos?
Es al contrario, los delitos informáticos se han incrementado, no existe una protección clara de contraseñas por parte d los usuarios y de este factor se aprovechan los ciberdelincuentes y robo de información para su posterior venta.

Pregunta 8: De acuerdo a su experiencia diga usted ¿Cuáles son las áreas específicas que deberían mejorarse en la Ley 30096 para abordar de manera más efectiva el incremento de la ciberdelincuencia?
Los responsables son la Policía Nacional del Perú y el Ministerio Público de enfrentar a estos ciberdelincuentes, pero la falta de recursos, financieros, personal y equipos afectan su labor de control de estos delincuentes.

Pregunta 9: En su opinión ¿Cuál sería la justificación legal más sólida para clasificar el phishing como delito y adoptar medidas preventivas contra la ciberdelincuencia?
La justificación legal de este delito es la causa de lesión al patrimonio de las personas que son sorprendidas por estos ciberdelincuentes y generan mayor conflicto en la sociedad.



FIRMA Y SELLO

Anexo 7 – Entrevista # 5

GUÍA DE ENTREVISTA

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

TÍTULO

“La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima norte 2022”

ENTREVISTADO/A : ROXANA ELIZABETH GENESIS CAJO PALACIOS

CARGO : ASISTENTE DE FUNCION FISCAL – LIMA NORTE

FECHA : 26 DE OCTUBRE DEL 2023

Las tecnologías de la información (TIC) han experimentado un crecimiento exponencial a nivel mundial gracias al internet. Esto ha facilitado la administración, procesamiento y compartición de información a través de diferentes dispositivos como computadoras, laptops, teléfonos móviles y televisores. Sin embargo, este avance ha dado lugar a la ciberdelincuencia, una modalidad de acciones ilícitas que se aprovecha de la dependencia de las personas en la tecnología para realizar diversas actividades.

El presente instrumento pretende recopilar su opinión respecto a este tema, en el cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales

Objetivo General

Identificar cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 1: A su criterio ¿Considera usted que los delitos del phishing deben ser incorporados y penalizados en nuestro sistema de justicia?

MONTADEUDAS, son un esquema de fraude y extorsión en el que se ofrecen prestamos con intereses excesivos y se utilizan amenazas para realizar los cobros. Dicho hecho se comete a través de las redes sociales y casa vez son más las víctimas.

Pregunta 2: A su criterio ¿Cuáles serían los elementos objetivos que deben ser considerados a fin de tipificar dichas conductas?
Elementos objetivos: que el agente activo, actúe mediante engaño, astucia y ardid a fin de que pueda ingresar a su patrimonio de la victima y hacer uso de ellos con el fin de ocasionar un detrimento a su patrimonio.
El agente activo, induce a error al agraviado, a fin de que este brinde datos, con el fin de que se le otorgue un préstamo bancario
Su accionar es netamente doloso.
Pregunta 3: En su opinión ¿Considera que es importante la tipificación de las modalidades como el Phishing, en nuestro ordenamiento jurídico?

OBJETIVO ESPECIFICO 1

Identificar cuáles son los elementos a considerarse para tipificar la conducta delictiva del phishing para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 4: En base a su experiencia ¿Qué naturaleza jurídica debe adoptar la tipificación de las conductivas del Phishing, de resultado o peligro?

Naturaleza de peligro, ya que su accionar produce un riesgo inmediato a su patrimonio.

Pregunta 5: En base a su experiencia diga usted ¿Cuáles son las modalidades más frecuentes en el Perú, para la comisión del delito de fraude informático?

- Interceptación de datos informáticos
- Trafico ilegal de datos

- Suplantación de identidad
- Abuso de mecanismo y dispositivos informáticos
- Fraude informático

Pregunta 6: A su criterio ¿La ciberdelincuencia se incrementa debido a falta de una ley adecuada?

Considero, que más que una ley adecuada, se propaga esta figura delictiva, por el libre acceso que se da en el ámbito cibernético, el mismo que no tienen parámetros estrictos. La ley como todas las leyes pueden poner parámetros, como en los delitos que ampara nuestro código penal, pero ellos no certifican que se erradique o deje de incrementar.

OBJETIVO ESPECIFICO 2

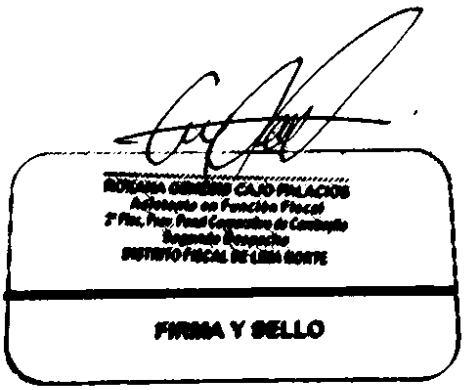
Determinar el aspecto jurídico a aplicarse para tipificar las conductas delictivas del phishing para prevenir de ciberdelincuencia Lima norte 2022.

Pregunta 7: En su opinión, desde la adhesión al Convenio de Budapest 2019 y la Ley n.º 30096, ¿El Perú ha podido minimizar los casos de Delitos informáticos?
Considero que anteriormente, no era tan propagada los delitos cibernéticos que en la actualidad se observan por ello no puedo evaluar una disminución, por el contrario en la actualidad si se observa eminentemente la gravedad de los delitos cibernéticos, los mismo que a mi apreciación , es por la libertad tecnológica y la recurrencia que los mismo usuarios otorgan al ámbito cibernético, el cual conforme se dé el avance de la tecnología y el apego que la sociedad le otorga, aun se aumentara y asimismo habrán otros delitos, opino que las restricciones a datos personales deben tener parámetros y así no aumentar el incremento de estos delitos

Pregunta 8: De acuerdo a su experiencia diga usted ¿Cuáles son las áreas específicas que deberían mejorarse en la Ley 30096 para abordar de manera más efectiva el incremento de la ciberdelincuencia?

Actualmente en artículo 207-A del código penal debería modificarse, con finalidad de mencionar todas las modalidades de delitos cibernéticos, con finalidad que las demandas penales a estos delincuentes sean más efectivas.

Pregunta 9: En su opinión ¿Cuál sería la justificación legal más sólida para clasificar el phishing como delito y adoptar medidas preventivas contra la ciberdelincuencia?
El agente pasivo a la vez de la figura del phishing, son figuras de alta jerarquía, toda vez que su identidad es suplantada a fin de solicitar a diferentes entidades que puedan permitir información personal de los usuarios, en ese sentido considero que esta figura debe ser amparada en protección legal, toda vez que acarrea una disminución patrimonial a los usuarios



Anexo 8 – Entrevista # 6

GUÍA DE ENTREVISTA

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

TÍTULO

"La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima norte 2022"

ENTREVISTADO/A : RAQUEL LAURA NUÑEZ COLQUEHUANCA

CARGO : ASISTENTE EN FUNCIÓN FISCAL LIMA NORTE

FECHA : 24 DE OCTUBRE DEL 2023

Las tecnologías de la información (TIC) han experimentado un crecimiento exponencial a nivel mundial gracias al internet. Esto ha facilitado la administración, procesamiento y compartición de información a través de diferentes dispositivos como computadoras, laptops, teléfonos móviles y televisores. Sin embargo, este avance ha dado lugar a la ciberdelincuencia, una modalidad de acciones ilícitas que se aprovecha de la dependencia de las personas en la tecnología para realizar diversas actividades.

El presente instrumento pretende recopilar su opinión respecto a este tema, en el cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales

Objetivo General

Identificar cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 1: A su criterio ¿Considera usted que los delitos del phishing deben ser incorporados y penalizados en nuestro sistema de justicia?

Sí, porque con el avance de la tecnología se han ido originando nuevas maneras de cometer hechos ilícitos, tal como phishing, que es una forma de fraude en línea que implica engañar a las personas, haciéndose pasar por instituciones confiables, a fin de obtener información confidencial de las tarjetas de crédito, tal como las contraseñas, números de tarjetas y demás detalles, siendo que dichos actos ocasionan daños financieros y personales a las víctimas, lo que ocasiona que las personas pierdan la confianza en las transacciones que se hacen a través del internet.

Pregunta 2: A su criterio ¿Cuáles serían los elementos objetivos que deben ser considerados a fin de tipificar dicha conducta?

Para que se configure el delito phishing, se debe tener presente los siguientes elementos objetivos: **i)** Suplantación de identidad, es decir, el autor del evento delictivo debe hacerse pasar por una entidad confiable tal como un banco u otra organización gubernamental. **ii)** Engaño o Fraude, esto es, la simulación de situaciones o sucesos de hechos materiales y psicológicos, para inducir a error a su víctima, pero dicho engaño debe ser idóneo o suficiente. **iii)** Medios electrónicos, los cuales deben ser utilizados para llevar a cabo el engaño en la víctima, como por ejemplo correo electrónico, página web, mensaje de texto u otro medio. **iv)** Obtención de la Información, aquí es cuando se consuma el delito mencionado, pues a través de los otros elementos antes mencionados, el autor del hecho ilícito logra obtener las contraseñas, cuentas de ahorro, los números de tarjeta, los usuarios entre otros. **v)** Daño patrimonial, es causado a consecuencia de la entrega de la información, ya que dicha información permite realizar los fraudes, hurto u otro delito.

Pregunta 3: En su opinión ¿Considera que es importante la tipificación de las modalidades como el Phishing, en nuestro ordenamiento jurídico?

Sí, es muy importante poder tipificar la comisión del delito de phishing, ya que va a permitir delimitar de manera clara las acciones que van a constituir el delito en mención, orientando a las autoridades del Poder Judicial, Ministerio Público y Policía Nacional del Perú poder investigar y perseguir los casos de phishing, facilitando la cooperación entre estas autoridades para luchar contra el crimen

cibernético, asimismo, dicha normativa va a disuadir a los autores de este tipo penal, permitiendo así la protección a la víctima.

OBJETIVO ESPECIFICO 1

Identificar cuáles son los elementos a considerarse para tipificar la conducta delictiva del phishing para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 4: En base a su experiencia ¿Qué naturaleza jurídica debe adoptar la tipificación de las conductivas del Phishing, de resultado o peligro?

La naturaleza jurídica del phishing, es de resultado, porque al obtener la información confidencial de las tarjetas de crédito débito, otras cuentas de ahorros u otra información personal y/o financiera, se configura el delito en mención, ya que después de obtener dicha información, lo que queda es el perjuicio patrimonial a la víctima, por lo que, el resultado especifico es esencial para que el delito se considere completo. Por último, el resultado del phishing no solo se refiere a la obtención de información, sino también a las posibles consecuencias negativas para la víctima, como la pérdida financiera y el riesgo de robo de identidad.

Pregunta 5: En base a su experiencia diga usted ¿Cuáles son las modalidades más frecuentes en el Perú, para la comisión del delito de fraude informático?

- El phishing, se da cuando los autores del delito envían correos electrónicos o mensajes de texto engañosos, que parecen ser confiables, a fin de obtener la información confidencial de la víctima y causarle un daño patrimonial.
- Suplantación de identidad, donde los autores del hecho delictivo suplantan la identidad de una persona o una entidad para engañar a otros usuarios.
- Fraude de criptomonedas, es cuando utilizan técnicas fraudulentas para engañar a las personas y robar las criptomonedas.
- Transferencias fraudulentas, se da cuando un equipo celular es arrebatado (hurto o robo), transfiriendo desde dicho equipo dinero de una cuenta que se encuentra guardada en el celular a las cuentas de los autores del hecho delictivo.

- Ransomware, implica un comportamiento delictivo en el que se emplea un software malicioso, que bloquea el acceso a los archivos de una computadora o red, exigiendo que ingrese un link, cuyo objetivo es tomar el control de los datos de la víctima y chantajearla a cambio.

Pregunta 6: A su criterio ¿La ciberdelincuencia se incrementa debido a falta de una ley adecuada?

En parte se debe a la falta de una legislación adecuada y efectiva para hacer frente a las amenazas digitales, pero también se debe a los diferentes avances de la tecnología que se incrementan diariamente.

OBJETIVO ESPECIFICO 2

Determinar el aspecto jurídico a aplicarse para tipificar las conductas delictivas del phishing para prevenir de ciberdelincuencia Lima norte 2022.

Pregunta 7: En su opinión, desde la adhesión al Convenio de Budapest 2019 y la Ley N.º 30096, ¿El Perú ha podido minimizar los casos de Delitos informáticos?

Considero que no se ha podido minimizar los casos de los delitos informáticos, debido a que los delitos informáticos evolucionan diariamente con el avance de las herramientas tecnológicas; sin embargo, no hay que menospreciar el esfuerzo que se hace en el Perú para poder minimizar la comisión de los delitos informáticos, puesto que vienen fortaleciendo las leyes y políticas en la ciberseguridad, invirtiendo en tecnología y sistemas de seguridad, además de realizar prácticas de prevención a fin de protegerse contra las amenazas cibernéticas.

Pregunta 8: De acuerdo a su experiencia diga usted ¿Cuáles son las áreas específicas que deberían mejorarse en la Ley 30096 para abordar de manera más efectiva el incremento de la ciberdelincuencia?

Para la mejora de dicha Ley se debe considerar diferentes factores, tales como el contexto legal, tecnológico y social, entre los cuales son las definiciones claras de las actividades que constituyen los delitos informáticos, además, de una adecuada pena o sanción que debe ser proporcional a la gravedad del delito, así también, se

debe mejorar la cooperación internacional, puesto que muchos de los delitos informáticos son cometidos en países distintos al Perú, lo que imposibilita la obtención de mayores elementos de convicción y medios probatorios que permitan resolver la participación y comisión de estos delitos.

Por otro lado, se debe implementar un proyecto de concientización y educación respecto a las amenazas cibernéticas que existen en nuestro país, que permita mejorar las prácticas en la protección de los datos e información personal, puesto que nuestro país se advierte que dichos datos son obtenidos de manera rápida y practica en los mercados negros, que venden las bases de datos, quienes también deberían ser penalizados, puesto que exponen información personal.

Pregunta 9: En su opinión ¿Cuál sería la justificación legal más sólida para clasificar el phishing como delito y adoptar medidas preventivas contra la ciberdelincuencia?

La justificación legal para clasificar el phishing como delito es la protección del bien jurídico, como lo es patrimonio, puesto que, al obtener la información confidencial de las tarjetas de crédito, débito, cuentas de ahorro u otras, a través del engaño idóneo a la víctima, le causa un daño patrimonial, pues el sujeto pasivo ve mellado su patrimonio, ya que les causan daños financieros y económicos, lo que produce una desconfianza en el uso de las páginas web o el propio internet, debiendo de adoptar las medidas contra los fraudes informáticos, como la educación y concientización de los medios electrónicos a usar, la protección de datos, como las contraseñas, número de cuentas de ahorros o de tarjetas, realizar la búsqueda de información en páginas de internet seguras y que las instituciones públicas o privadas tengas políticas de seguridad y confidencialidad.

Anexo 9 – Entrevista # 7

GUÍA DE ENTREVISTA

INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

TÍTULO

"La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima norte 2022"

ENTREVISTADO/A : DARWIN DARIO CARI HUACCACHI

CARGO : ASISTENTE ADMINISTRATIVO

FECHA : 27 DE OCTUBRE DEL 2023

Las tecnologías de la información (TIC) han experimentado un crecimiento exponencial a nivel mundial gracias al internet. Esto ha facilitado la administración, procesamiento y compartición de información a través de diferentes dispositivos como computadoras, laptops, teléfonos móviles y televisores. Sin embargo, este avance ha dado lugar a la ciberdelincuencia, una modalidad de acciones ilícitas que se aprovecha de la dependencia de las personas en la tecnología para realizar diversas actividades.

El presente instrumento pretende recopilar su opinión respecto a este tema, en el cual se pide responder las siguientes preguntas con neutralidad y precisión, sin ser necesario el uso de citas textuales

Objetivo General

Identificar cuáles son los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 1: A su criterio ¿Considera usted que los delitos del phishing deben ser incorporados y penalizados en nuestro sistema de justicia?

De acuerdo, deben ser considerado en el sistema jurídico peruano, considerando además que el artículo 207-A es muy genérico al respecto, no considera nuevas modalidades que los ciberdelincuentes aprovechan como el pharming y carding.

Pregunta 2: A su criterio ¿Cuáles serían los elementos objetivos que deben ser considerados a fin de tipificar dichas conducta?
Se debe de tener en cuenta que los elementos sería el usar medios informáticos a través de los cuales se suplanta la identidad de una persona, con finalidad de sustraer información confidencial para vulnerar elementos que serán tipificados como delitos.

Pregunta 3: En su opinión ¿Considera que es importante la tipificación de las modalidades como el Phishing, en nuestro ordenamiento jurídico?

Totalmente de acuerdo, ya se adelantó opinión al respecto debido al delito penal que se le atribuye.

OBJETIVO ESPECIFICO 1
Identificar cuáles son los elementos a considerarse para tipificar la conducta delictiva del phishing para prevenir la ciberdelincuencia Lima norte 2022

Pregunta 4: En base a su experiencia ¿Qué naturaleza jurídica debe adoptar la tipificación de las conductivas del Phishing, de resultado o peligro?

Es considerado como un modo de delito de tipo penal, considerado de asunto de peligro.

Pregunta 5: En base a su experiencia diga usted ¿ Cuáles son las modalidades más frecuentes en el Perú, para la comisión del delito de fraude informático?

Las modalidades serían las siguientes: en primer lugar las páginas clonadas falsas, mediante el phishing, donde las ciberdelincuencias engañan a usuarios con paginas falsas simulando ser sitios web de entidades financieras o bancarias. En

segundo; termino, las compras fraudulentas usando las tarjetas de clientes clonadas y estafando en entidades comerciales y/o bancarias.

Pregunta 6: A su criterio ¿La ciberdelincuencia se incrementa debido a falta de una ley adecuada?

Existe una falta de los usuarios de los medios virtuales, al no tener páginas web con claves más rígidas e ingresar a plataformas no confiables, de esto se aprovecha la ciberdelincuencia para seguir estafando en las redes sociales, por la necesidad de seguir estafando a usuarios.

OBJETIVO ESPECIFICO 2

Determinar el aspecto jurídico a aplicarse para tipificar las conductas delictivas del phishing para prevenir de ciberdelincuencia Lima norte 2022.

Pregunta 7: En su opinión, desde la adhesión al Convenio de Budapest 2019 y la Ley n.º 30096, ¿El Perú ha podido minimizar los casos de Delitos informáticos?
En el aspecto legal existe un crecimiento de las autoridades en enfrentar este delito, como la Policía Nacional del Perú y el Ministerio Público, pero siempre la falta de presupuesto que se les puede asignar generan falta de recursos para enfrentar a los ciberdelincuentes.

Pregunta 8: De acuerdo a su experiencia diga usted ¿Cuáles son las áreas específicas que deberían mejorarse en la Ley 30096 para abordar de manera más efectiva el incremento de la ciberdelincuencia?
En la actualidad considerando el incremento del uso frecuente de redes informática y la información electrónica para cometer delitos, es muy oportuno que las entidades que brindar servicios financieros o bancarios, tengan protocolos de seguridad mayores para evitar estas estafas.

Pregunta 9: En su opinión ¿Cuál sería la justificación legal más sólida para clasificar el phishing como delito y adoptar medidas preventivas contra la ciberdelincuencia?

El perjuicio muy recurrente, es la sensación de impunidad en los juicios, por falta de regulación clara donde se describa el tipo penal y la sanción ejemplar.

Anexo 10 – Ficha de análisis de fuente de documentos.

FICHA DE ANÁLISIS DE FUENTE DE DOCUMENTOS

INSTRUMENTO DE RECOLECCIÓN DE DATOS

FICHA DE ANÁLISIS DE FUENTE DE DOCUMENTOS

Título de la investigación

“La tipificación del phishing en nuestro sistema penal peruano, y la prevención de ciberdelincuencia, Lima norte 2022”

Objetivo General

Identificar los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima Norte 2022

I. ANALISIS DE ARTICULO

<table>
<tr><td colspan="2">Ficha de análisis de fuente de documentos – Resolución Presidencial</td></tr>
<tr><td colspan="2">Identificación de la fuente:
Zelada (2021) su artículo “Delitos informáticos ¿Nuevas formas de criminalidad?”
Link: https://www.deleyes.pe/articulos/delitos-informaticos-nuevas-formas-de-criminalidad</td></tr>
<tr><td>Texto relevante</td><td>Análisis del Contenido</td></tr>
<tr><td>Mencionó en su investigación, que la ley 30096 sobre delitos informáticos busca prevenir y a la vez sancionar este tipo de acciones ilícitas que afectan los sistemas y datos de empresas jurídica y personas naturales</td><td>Desde marzo del 2020 hasta la fecha, nos enfrentamos a un nuevo modo de adquisición de activos, pago de servicios e incluso formas de trabajo. Esta “evolución” hacia el mundo informático y virtual ha aportado muchos beneficios. Sin embargo, también ha generado innumerables dificultades. Uno de los problemas más relevantes y
significativos son las actividades delictivas cometidas a través de los sistemas</td></tr>
</table>

	informáticos, las cuales han sido debidamente reguladas por nuestro legislador nacional en la Ley 30096, Ley de Delitos Informáticos, modificada por la Ley 30171
Ponderamiento	
A manera de conclusión: Los presupuestos especiales de los delitos informáticos permiten establecer una relación directa con la criminalidad económica, que no solamente se circunscribe a delitos patrimoniales, sino que también engloba tipos penales que cuentan con una importante repercusión en el sistema informático y, accesoriamente, en el sistema económico.	

Objetivo General:

Identificar los fundamentos jurídicos para tipificar el phishing en el sistema penal peruano para prevenir la ciberdelincuencia Lima Norte 2022

I. ANALISIS DE ARTICULO DE INVESTIGACION

<table>
<tr><td colspan="2">Ficha de análisis de fuente de documentos – Articulo de Investigación</td></tr>
<tr><td colspan="2">Identificación de la fuente:
Castañeda et al. (2021) “Vista de los delitos cibernéticos en Chile, México y Colombia”

Link: https://iuscomitialis.uaemex.mx/article/view/17320/12891</td></tr>
<tr><td>Texto relevante</td><td>Análisis del Contenido</td></tr>
<tr><td>Su artículo tuvo por finalidad el analizar los delitos cibernéticos en los países de México, Colombia y Chile para que puedan estudiar los ordenamientos jurídicos de estas nuevas formas de delitos y ver los avances con respecto al Convenio sobre Ciberdelincuencia 2001 firmado en Budapest.</td><td>Enfocaron como la ciberdelincuencia en México se ha multiplicado especialmente por el desarrollo de las herramientas tecnológicas de la información, que las entidades bancarias y comerciales han desarrollado con finalidad de promocionar sus productos y servicios, y que estas son aprovechadas por organizaciones criminales que a través de malware y spam sorprenden a las personas, con lo cual utilizan los datos de otras personas y afectando su economía y reputación.</td></tr>
<tr><td colspan="2">Ponderamiento</td></tr>
<tr><td colspan="2">A manera de conclusión: Concluyeron, que los países involucrados a la fecha tienen leyes que sancionan la ciberdelincuencia, pero no aplican de acuerdo a lo requerido por la Convención sobre la Ciberdelincuencia que ocurre en Chile y México, porque no han modernizado su legislación para una sanción más tipificada a los nuevos instrumentos de delincuencia cibernética como son el phishing, smishing, vishing, entre otros.</td></tr>
</table>

Objetivo específico 1:
Identificar los elementos que se deben de tener en cuenta para tipificar la conducta delictiva del phishing para la prevención de ciberdelincuencia Lima Norte 2022

I. ANALISIS DE ARTICULO DE INVESTIGACION

<table>
<tr><td colspan="2">Ficha de análisis de fuente de documentos – Articulo de Investigación</td></tr>
<tr><td colspan="2">Identificación de la fuente:
Sviatun et al. (2021) “Combating cybercrime: Economic and legal aspects”

Link:
https://www.researchgate.net/publication/351740010_Combating_Cybercrime_Economic_and_Legal_Aspects</td></tr>
<tr><td>Texto relevante</td><td>Análisis del Contenido</td></tr>
<tr><td>consideraron en su investigación que el cibercrimen amenaza la seguridad nacional de diferentes países del mundo. El crecimiento de los ciberataques desestabiliza el orden internacional y trastorna el normal funcionamiento de las relaciones internacionales</td><td>Su propósito del artículo académico es analizar las causas y las consecuencias económicas del nivel de ciberdelincuencia en el mundo e identificar los arreglos legales modernos para combatir la ciberdelincuencia. Para lograr este propósito planteado, han utilizado los siguientes métodos, a saber: el método de comparación, análisis, método teórico-elemental, método de generalización y analogía.</td></tr>
<tr><td colspan="2">Ponderamiento</td></tr>
<tr><td colspan="2">A manera de conclusión: Establecieron que el nivel de ciberdelincuencia en el mundo y las consecuencias económicas de su impacto tienden a aumentar. Se estima que en 2020 el costo total del cibercrimen y la ciberseguridad superará el billón de dólares estadounidenses, lo que representa más del 1 % del producto interno bruto mundial.</td></tr>
</table>

Objetivo específico 1:
Identificar los elementos que se deben de tener en cuenta para tipificar la conducta delictiva del phishing para la prevención de ciberdelincuencia Lima Norte 2022

I. ANALISIS DE ARTICULO DE INVESTIGACION

<table>
<tr><td colspan="2">Ficha de análisis de fuente de documentos – Articulo de Investigación</td></tr>
<tr><td colspan="2">Identificación de la fuente:
Macías et al. (2022) “Frequent cases, criminalization and prevention of computer crimes in Ecuador”

Link: https://journals.sapienzaeditorial.com/index.php/SIJIS/article/view/324</td></tr>
<tr><td>Texto relevante</td><td>Análisis del Contenido</td></tr>
<tr><td>Determinaron en su investigación, que los delitos informáticos a nivel mundial y en el Ecuador se han incrementado en forma exponencial a partir del año 2020.</td><td>Donde indicaron que se menciona en los periódicos, revistas, noticias de radio y programas periodísticos que los casos más numéricos son la suplantación de identidad, falsificación de documentos, apropiación fraudulenta por medios electrónicos, ataques a sistemas informáticos, interceptación ilegal de datos, transferencia electrónica sin consentimiento y revelación ilegal de datos.</td></tr>
<tr><td colspan="2">Ponderamiento</td></tr>
<tr><td colspan="2">A manera de conclusión: Todos estos casos son relevantes en la sociedad ecuatoriana, y las leyes establecidas no han reducido los mismos, debido a que los ciberdelincuentes no tienen temor a sus acciones ilegales que realizan, debido a que sus métodos cada vez son más desarrollados y difíciles de ubicar.</td></tr>
</table>

Objetivo específico 2:

Determinar la naturaleza jurídica que se debe considerar para tipificar la conducta delictiva del phishing como prevención de ciberdelincuencia Lima Norte 2022

I. ANALISIS DE ARTICULO DE INVESTIGACION

<table>
<tr><td colspan="2">Ficha de análisis de fuente de documentos – Articulo de Investigación</td></tr>
<tr><td colspan="2">Identificación de la fuente:
Ramirez et al. (2022) “Validation of a cybercrime awareness scale in Peruvian university students”

Link: http://www.scielo.org.co/pdf/recig/v20n37/2500-7645-recig-20-37-208.pdf</td></tr>
<tr><td>Texto relevante</td><td>Análisis del Contenido</td></tr>
<tr><td>Investigación que realizaron fue determinar como la conciencia en estudiantes universitarios, sobre la identificación de los principales indicadores sobre los cibercrímenes en nuestra sociedad y enumerarlos de acuerdo a su importancia,</td><td>Aplicaron un estudio a 372 estudiantes mediante encuestas por Google Form, las respuestas son: 1) conciencia sobre phishing, 2) conciencia sobre el spamming, 3) eficacia del software antivirus, y 4) bullying en la web.</td></tr>
<tr><td colspan="2">Ponderamiento</td></tr>
<tr><td colspan="2">A manera de conclusión: Concluyeron, que los estudiantes universitarios tienen conocimiento de los modelos de cibercrimen que existen, y consideran que la sociedad debe ser capacitada ante los engaños fraudulentos de estas organizaciones dirigidas por criminales con alto conocimiento de sistemas.</td></tr>
</table>

Objetivo específico 2:

Determinar la naturaleza jurídica que se debe considerar para tipificar la conducta delictiva del phishing como prevención de ciberdelincuencia Lima Norte 2022.

I. ANALISIS DE ARTICULO DE INVESTIGACION

<table>
<tr><td colspan="2">Ficha de análisis de fuente de documentos – Articulo de Investigación</td></tr>
<tr><td colspan="2">Identificación de la fuente:
Vinelli (2021) Los delitos informáticos y su relación con la criminalidad económica”

Link:
https://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/download/4995/5428/</td></tr>
<tr><td>Texto relevante</td><td>Análisis del Contenido</td></tr>
<tr><td>En la investigación que realizaron han identificado las actividades delictivas cometidas a través de los sistemas informáticos, las cuales han sido debidamente reguladas por nuestro legislador nacional en la Ley 30096, Ley de Delitos Informáticos, modificada por la Ley 30171.</td><td>Aplicaron un estudio a 372 estudiantes mediante encuestas por Google Form, las respuestas son: 1) conciencia sobre phishing, 2) conciencia sobre el spamming, 3) eficacia del software antivirus, y 4) bullying en la web.</td></tr>
<tr><td colspan="2">Ponderamiento</td></tr>
<tr><td colspan="2">A manera de conclusión: Concluyeron, han identificado las actividades delictivas cometidas a través de los sistemas informáticos, las cuales han sido debidamente reguladas por nuestro legislador nacional en la Ley 30096, Ley de Delitos Informáticos, modificada por la Ley 30171..</td></tr>
</table>

Anexo 11- Matriz de validación de expertos

Evaluación por juicio de expertos

Respetado Juez: Usted ha sido seleccionado para evaluar el instrumento de "Guía de entrevista". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al que hacer jurídico. Agradecemos su valiosa colaboración.

1. Datos generales del juez:

Nombre completo:	UBALDO CALLO DEZA
Grado profesional:	Maestría ( ) Doctor (**X**)
Área de formación académica:	Clínica ( ) Social ( ) Educativa (**X**) Organizacional ( )
Áreas de experiencia profesional:	Docente Universitario
Institución donde labora:	Universidad César Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (**X**)
Experiencia en Investigación Jurídica: (si corresponde)	

1. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

2. Datos de la escala (Técnica de la entrevista)

Nombre de la Prueba:	Guía de entrevista
Autor(a):	Barahona Rojas Vanessa Josselin
Procedencia:	Lima - Perú
Administración:	Propia
Tiempo de aplicación:	60 minutos
Ámbito de aplicación:	Lima norte
Significación:	La investigación tiene como categoría 1: Tipificación del phishing en el sistema penal peruano, con subcategorías: Ley No. 30096 - Delitos informáticos. Proceso judicial: casos de ciberdelincuencia; como categoría 2: Prevención de ciberdelincuencia, con subcategorías (1) Administración de Justicia (2) División de Investigación de delitos de Alta Tecnología.

3. Soporte teórico (describir en función al modelo teórico)

Escala/ÁREA	Sub categorías	Definición
La tipificación del phishing en nuestro sistema penal peruano	(3) Ley No. 30096 - Delitos informáticos. (4) Proceso judicial: casos de ciberdelincuencia.	En el Perú se aprobó la Ley 30096 (2013) denominada ley de delitos informáticos y modifica en algunos artículos en la ley 30171 publicada en marzo del 2014, la cual se encuentra relacionada sobre Convenio sobre la Ciberdelincuencia de Budapest del año 2001.

Prevención de ciberdelincuencia	(3) Administración de Justicia (2) División de Investigación de delitos de Alta Tecnología.	Benavides et al. (2020) el phishing es conocido como una combinación de ingeniera y exploits técnicos, a través de los cuales convencen a las personas en proporcionar sus claves o datos personales para acceder a sus diversas cuentas personales en entidades bancarias, financieras y comerciales.

4. <u>Presentación de instrucciones para el juez</u>:

A continuación, a usted le presento la guía de entrevista elaborada por **Barahona Rojas Vanessa Josselin** en el año 2023. De acuerdo con los siguientes indicadores a fin de que califique cada uno de los ítems según corresponda.

Categoría	**Calificación**	**Indicador**
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.

estámidiendo.	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (altonivel)	El ítem se encuentra está relacionado con ladimensión que está midiendo.
RELEVANCIA El ítem es esencialo importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se veaafectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítempuede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1. No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Categorías y subcategorías del instrumento:

Categorías	Subcategorías
Categoría 1: tipificación del phishing en nuestro sistema penal peruano	(1) Ley No. 30096 - Delitos informáticos. (2) Proceso judicial: casos de ciberdelincuencia.
Categoría 2: prevención de la ciberdelincuencia lima norte 2022	(1) Administración de Justicia (2) División de Investigación de delitos de Alta Tecnología.

- Objetivos de las Categorías y subcategorías: Recabar información de los expertos

especialistas en la **delación premiada**, así como **el juicio justo** con la finalidad de lograr el objeto de estudio, consiguientemente generar teorías emergentes pertinente al estudio.

Indicadores	**Ítem**	**Claridad**	**Coherencia**	**Relevancia**	**Observaciones/ Recomendaciones**
Tipificar el phishing en el sistema penal peruano	1	4	4	4	
Importancia para que el congreso modifique la ley 30096	2	4	4	4	
phishing	3	4	4	4	
Elementos a considerar para tipificar el phishing	4	4	4	4	
Elementos que deben estar presentes para tipificar la conducta delictiva del phishing	5	4	3	4	
Incremento de la ciberdelincuencia debido a falta de una ley adecuada	6	4	4	3	
Importancia para tipificar el phishing como una conducta delictiva	7	4	4	4	
Mejorar la ley 30096	8	4	3	4	

Razones para tipificar el phishing y prevenir la ciberdelincuencia	9	4	4	4	

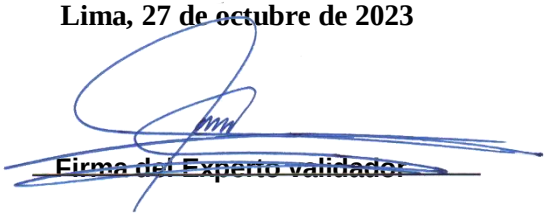
Observaciones (precisar si hay suficiencia):
_____
_____

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Callo Deza Ubaldo

Especialidad del validador: Docente Universitario

Lima, 27 de octubre de 2023



Firma del Experto validador:

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Evaluación por juicio de expertos

Respetado Juez: Usted ha sido seleccionado para evaluar el instrumento de "Guía de entrevista". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al que hacer jurídico. Agradecemos su valiosa colaboración.

1. Datos generales del juez:

Nombre completo:	Mg. Arosemena Angulo Agustín Nicolas
Grado profesional:	Maestría (x) Doctor ( )
Área de formación académica:	Clínica ( ) Social () Educativa (X) Organizacional ( )
Áreas de experiencia profesional:	Docente Universitario
Institución donde labora:	Universidad César Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (**X**)
Experiencia en Investigación Jurídica: (si corresponde)	

5. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

6. Datos de la escala (Técnica de la entrevista)

Nombre de la Prueba:	Guía de entrevista
Autor(a):	Barahona Rojas Vanessa Josselin
Procedencia:	Lima - Perú
Administración:	Propia
Tiempo de aplicación:	60 minutos
Ámbito de aplicación:	Lima norte
Significación:	La investigación tiene como categoría 1: Tipificación del phishing en el sistema penal peruano, con subcategorías (1) Ley No. 30096 - Delitos informáticos. (2) Proceso judicial: casos de ciberdelincuencia.; como categoría 2, y sub categorías (1) Administración de Justicia (2) División de Investigación de delitos de Alta Tecnología.

7. Soporte teórico (describir en función al modelo teórico)

Escala/ÁREA	Sub categorías	Definición
La tipificación del phishing en nuestro sistema penal peruano	**(1) Ley No. 30096 -Delitos informáticos.** **(2) Proceso judicial: casos de ciberdelincuencia.**	En el Perú se aprobó la Ley 30096 (2013) denominada ley de delitos informáticos y modifica en algunos artículos en la ley 30171 publicada en marzo del 2014, la cual se encuentra relacionada sobre Convenio sobre la Ciberdelincuencia de Budapest del año 2001.

Prevención de ciberdelincuencia	**(1)Administración de Justicia** **(2) División de Investigación de delitos de Alta Tecnología.**	Benavides et al. (2020) el phishing es conocido como una combinación de ingeniera y exploits técnicos, a través de los cuales convencen a las personas en proporcionar sus claves o datos personales para acceder a sus diversas cuentas personales en entidades bancarias, financieras y comerciales.

8. <u>Presentación de instrucciones para el juez</u>:

A continuación, a usted le presento la guía de entrevista elaborada por **Barahona Rojas Vanessa Josselin** en el año 2023. De acuerdo con los siguientes indicadores a fin de que califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.

estámidiendo.	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (altonivel)	El ítem se encuentra está relacionado con ladimensión que está midiendo.
RELEVANCIA El ítem es esencialo importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se veaafectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítempuede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brindesus observaciones que considere pertinente

1. No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Categorías y subcategorías del instrumento:

Categorías	Subcategorías
Categoría 1: tipificación del phishing en nuestro sistema penal peruano	(1) Ley No. 30096 - Delitos informáticos. (2) Proceso judicial: casos de ciberdelincuencia.
Categoría 2: prevención de la ciberdelincuencia lima norte 2022	(1) Administración de Justicia (2) División de Investigación de delitos de Alta Tecnología..

- Objetivos de las Categorías y subcategorías: Recabar información de los expertos

especialistas en la **delación premiada**, así como **el juicio justo** con la finalidad de lograr el objeto de estudio, consiguientemente generar teorías emergentes pertinente al estudio.

Indicadores	**Ítem**	**Claridad**	**Coherencia**	**Relevancia**	**Observaciones/ Recomendaciones**
Tipificar el phishing en el sistema penal peruano	1	4	4	4	
Importancia para que el congreso modifique la ley 30096	2	4	4	4	
phishing	3	4	4	4	
Elementos a considerar para tipificar el phishing	4	4	4	4	
Elementos que deben estar presentes para tipificar la conducta delictiva del phishing	5	4	3	3	
Incremento de la ciberdelincuencia debido a falta de una ley adecuada	6	4	4	3	
Importancia para tipificar el phishing como una conducta delictiva	7	4	4	4	
Mejorar la ley 30096	8	4	3	4	

Razones para tipificar el phishing y prevenir la ciberdelincuencia	9	4	4	4	

Observaciones (precisar si hay suficiencia):
_____
_____

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

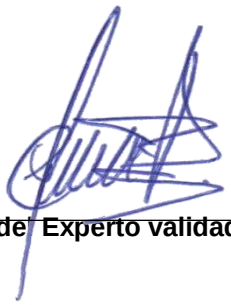
Apellidos y nombres del juez validador: Mg. Arosemena Angulo Agustín Nicolas

Especialidad del validador: Docente Universitario

Lima, 27 de octubre de 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión



Firma del Experto validador

Evaluación por juicio de expertos

Respetado Juez: Usted ha sido seleccionado para evaluar el instrumento de "Guía de entrevista". La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al que hacer jurídico. Agradecemos su valiosa colaboración.

1. Datos generales del juez:

Nombre completo:	Mg. Aguirre Rojas Levi Joel
Grado profesional:	Maestría (x) Doctor ( )
Área de formación académica:	Clínica ( ) Social (x) Educativa ( ) Organizacional ( )
Áreas de experiencia profesional:	Docente Universitario
Institución donde labora:	Universidad César Vallejo
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (**X**)
Experiencia en Investigación Jurídica: (si corresponde)	

9. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

10. <u>Datos de la escala</u> (Técnica de la entrevista)

Nombre de la Prueba:	Guía de entrevista
Autor(a):	Barahona Rojas Vanessa Josselin
Procedencia:	Lima - Perú
Administración:	Propia
Tiempo de aplicación:	60 minutos
Ámbito de aplicación:	Lima norte
Significación:	La investigación tiene como categoría 1: Tipificación del phishing en el sistema penal peruano, con subcategorías: (1) Ley No. 30096 - Delitos informáticos. (2) Proceso judicial: casos de ciberdelincuencia.; como categoría 2: Prevención de ciberdelincuencia, con subcategorías. (1) Administración de Justicia (2) División de Investigación de delitos de Alta Tecnología.

11. <u>Soporte teórico</u> (describir en función al modelo teórico)

Escala/ÁREA	Sub categorías	Definición
La tipificación del phishing en nuestro sistema penal peruano	**(1) Ley No. 30096 - Delitos informáticos.** **(2) Proceso judicial: casos de ciberdelincuencia**	En el Perú se aprobó la Ley 30096 (2013) denominada ley de delitos informáticos y modifica en algunos artículos en la ley 30171 publicada en marzo del 2014, la cual se encuentra relacionada sobre Convenio sobre la Ciberdelincuencia de Budapest del año 2001.

Prevención de ciberdelincuencia	(1) Administración de Justicia (2) División de Investigación de delitos de Alta Tecnología.	Benavides et al. (2020) el phishing es conocido como una combinación de ingeniera y exploits técnicos, a través de los cuales convencen a las personas en proporcionar sus claves o datos personales para acceder a sus diversas cuentas personales en entidades bancarias, financieras y comerciales.

12. <u>Presentación de instrucciones para el juez</u>:

A continuación, a usted le presento la guía de entrevista elaborada por **Barahona Rojas Vanessa Josselin** en el año 2023. De acuerdo con los siguientes indicadores a fin de que califique cada uno de los ítems según corresponda.

Categoría	**Calificación**	**Indicador**
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.

estámidiendo.	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (altonivel)	El ítem se encuentra está relacionado con ladimensión que está midiendo.
RELEVANCIA El ítem es esencialo importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se veaafectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítempuede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

Leer con detenimiento los ítems y calificar en una escala de 1 a 4 su valoración, así como solicitamos brinde sus observaciones que considere pertinente

1. No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel

Categorías y subcategorías del instrumento:

Categorías	Subcategorías
Categoría 1: tipificación del phishing en nuestro sistema penal peruano	(1) Ley No. 30096 - Delitos informáticos. (2) Proceso judicial: casos de ciberdelincuencia
Categoría 2: prevención de la ciberdelincuencia lima norte 2022	(1) Administración de Justicia (2) División de Investigación de delitos de Alta Tecnología.

- Objetivos de las Categorías y subcategorías: Recabar información de los expertos especialistas en la **delación premiada**, así como **el juicio justo** con la finalidad de lograr el objeto de estudio, consiguientemente generar teorías emergentes pertinente al estudio.

Indicadores	**Ítem**	**Claridad**	**Coherencia**	**Relevancia**	**Observaciones/ Recomendaciones**
Tipificar el phishing en el sistema penal peruano	1	4	4	4	
Importancia para que el congreso modifique la ley 30096	2	4	4	4	
phishing	3	4	4	4	
Elementos a considerar para tipificar el phishing	4	4	4	4	
Elementos que deben estar presentes para tipificar la conducta delictiva del phishing	5	4	3	3	
Incremento de la ciberdelincuencia debido a falta de una ley adecuada	6	4	4	3	
Importancia para tipificar el phishing como una conducta	7	4	4	4	

delictiva					
Mejorar la ley 30096	8	4	3	4	
Razones para tipificar el phishing y prevenir la ciberdelincuencia	9	4	4	4	

Observaciones (precisar si hay suficiencia): _____

_____

Opinión de aplicabilidad: Aplicable [X] Aplicable después de corregir [ ] No aplicable [ ]

Apellidos y nombres del juez validador: Mg. Aguirre Rojas Levi Joel

Especialidad del validador: Docente Universitario

Lima, 27 de octubre de 2023

[1]**Pertinencia:** El ítem corresponde al concepto teórico formulado.
[2]**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo
[3]**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión

Firma del Experto validador