



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

**La tipificación del Phishing en el sistema Penal peruano, para la lucha contra
la ciberdelincuencia**

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTOR:

Peralta Huaman, Alex Jaime (orcid.org/0000-0002-1532-8397)

ASESOR:

Mgtr. Riveros Tolentino, Edy Leonardo (orcid.org/0000-0002-6556-569X)

LÍNEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Enfoque de género, inclusión social y diversidad cultural

LIMA – PERÚ

2024



Declaratoria de Autenticidad del Asesor

Yo, RIVEROS TOLENTINO EDY LEONARDO, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, asesor de Tesis titulada: "LA TIPIFICACIÓN DEL PHISHING EN EL SISTEMA PENAL PERUANO, PARA LA LUCHA CONTRA LA CIBERDELINCUENCIA.", cuyo autor es PERALTA HUAMAN ALEX JAIME, constato que la investigación tiene un índice de similitud de 17%, 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, 01 de Julio del 2024

Apellidos y Nombres del Asesor:	Firma
RIVEROS TOLENTINO EDY LEONARDO DNI: 40541981 ORCID: 0000-0002-6556-569X	Firmado electrónicamente por: ERIVEROSTOL el 02-07-2024 07:07:16

Código documento Trilce: TRI - 0786218



**FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO**

Declaratoria de Originalidad del Autor

Yo, PERALTA HUAMAN ALEX JAIME estudiante de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ATE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "LA TIPIFICACIÓN DEL PHISHING EN EL SISTEMA PENAL PERUANO, PARA LA LUCHA CONTRA LA CIBERDELINCUENCIA.", 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
ALEX JAIME PERALTA HUAMAN DNI: 70037520 ORCID: 0000-0002-1532-8397	Firmado electrónicamente por: APERALTAH el 01-07- 2024 19:10:54

Código documento Trilce: TRI - 0786220

Dedicatoria

La presente tesis es dedicada a mi familia por su apoyo constante, por motivarme a seguir luchando por mis sueños.

A mis Padres, hermanos y seres queridos por su valioso aporte en el proceso de mi formación académica.

Agradecimiento

Agradezco a Dios por sobre todas las cosas, por haberme permitido culminar de forma satisfactoria la presente tesis.

Al Doctor Riveros, Edy por su apoyo constante en la elaboración de la presente tesis.

Índice de contenidos

Pág.

declaratoria de autenticidad del asesor	ii
declaratoria de originalidad del autor/ autores	iii
Dedicatoria	iv
Agradecimiento	v
índice de contenidos	vi
índice de tablas	vii
Resumen	viii
Abstract	ix
I. INTRODUCCIÓN	1
II. METODOLOGÍA	10
III. RESULTADOS	15
IV. DISCUSIÓN	27
V. CONCLUSIONES	33
VI. RECOMENDACIONES	35
REFERENCIAS	36
ANEXOS	

índice de tablas

	Pág.	
Tabla 1	Tabla de categorización	11
Tabla 2	Participantes	12
Tabla 3	Validez de Instrumento: Guía de Entrevista	13
Tabla 4	Validez de Instrumento: documento de análisis normativo	13
Tabla 5	Validez de Instrumento: documento de análisis doctrinario	13
Tabla 6	Validez de Instrumento: documento de análisis de derecho comparado	13
Tabla 7	Análisis normativo legal	16
Tabla 8	Resultados del objetivo específico 1	18
Tabla 9	Normativa Doctrinaria	20
Tabla 10	Resultados del objetivo específico 2	22
Tabla 11	Derecho comparado	23
Tabla 12	Resultados del objetivo específico 3	25
Tabla 13	Resultado final de la tesis	26

Resumen

La presente tesis, tuvo como objetivo general cuál es la Actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024, Asimismo tuvo como objetivos específicos: O.E 1, Explicar desde el aspecto normativo legal es la actualidad jurídica, 2024. O.E.2, Explicar desde el aspecto doctrinario es la actualidad jurídica, O.E.3, Explicar desde el derecho comparado es la actualidad jurídica. Para cuyo efecto se recurrió al enfoque cualitativo, con tipo de estudio básica, diseño de investigación perteneció a la teoría fundamentada. El presente trabajo de investigación como principal resultado fue que el escenario legal del Phishing informático en nuestro sistema penal peruano es desfavorable y ello se debe a: Primero, por su falta de regulación normativa, ya que los artículos comprendidos en la ley de delitos informáticos no contemplan esta figura delictiva del phishing si no como fraude. Segundo, la ley de delitos informáticos no consagra este tipo de modalidad que es más compleja toda vez que posee actos preparatorios para la comisión de ilícitos penales, causando perjuicio económico a las personas que son víctimas de estos ilícitos toda vez que no se puede imputar este tipo de delitos a los sujetos activos que comenten esta modalidad delictiva.

Palabras clave: Delitos informáticos, Phishing, ciberdelincuencia informática

Abstract

The general objective of this thesis was the current legal status of phishing in the Peruvian criminal system, for the fight against cybercrime, 2024. It also had the specific objectives: O.E 1, Explain from the legal regulatory aspect the current legal status, 2024.O.E.2, Explaining from the doctrinal aspect is the legal news, O.E.3, Explaining from comparative law is the legal news. For this purpose, the qualitative approach was used, with a basic type of study, the research design belonged to the grounded theory. The main result of this research work was that the legal scenario of computer phishing in our Peruvian criminal system is unfavorable and this is due to: First, due to its lack of regulatory regulation, since the articles included in the computer crime law do not They consider this criminal figure of phishing if not as fraud. Second, the computer crime law does not enshrine this type of modality, which is more complex since it has preparatory acts for the commission of criminal offenses, causing economic damage to the people who are victims of these crimes since this crime cannot be charged. type of crimes to active subjects who commit this type of crime.

Keywords: Computer crimes, Phishing, cybercrime.

I. INTRODUCCIÓN

En cuanto a la **realidad problemática**, los crímenes cibernéticos continúan evolucionando constantemente, ello se debe a la era tecnológica, este avance es positivo para el desarrollo de la industria, sin embargo, también trajo consigo el surgimiento de ilícitos penales que se adecuaron a las nuevas tecnologías, en ese sentido la era tecnológica ha traído consigo que los delincuentes informáticos tengan mayor acceso a la impunidad por falta de legislación uniforme respecto a los delitos informáticos. Por ello los índices de criminalidad informática tienen la más alta tasa de incidencia delictiva, situación que pone en riesgo a los usuarios quienes por carecer de conocimiento tecnológico. Son víctimas de los denominados ciberdelincuentes. Tomando en consideración ello debemos precisar que actualmente, nuestras actividades cotidianas se desarrollan a través de medios tecnológicos, sirviendo como medio para que delincuentes puedan cometer las distintas modalidades delictivas, causando perjuicio económico principalmente a los usuarios que por desconocimiento acceden a este tipo de fraude. En ese sentido, con el objetivo de hacerle frente a las nuevas tipologías criminales a nivel internacional varios estados han suscrito el convenio de Budapest y nuestro país no ha sido la excepción. De esta manera se debe de tomar en consideración el nacimiento de nuevas formas de ilícitos que se desarrollan en el espacio tecnológico.

Ante la aparición de estas nuevas modalidades a nivel internacional los estados han unido esfuerzos para enfrentar estos delitos que se desarrollan a través de medios tecnológicos. Por ello surgió como alternativa de solución el convenio de Budapest incluye a diversos países de Sudamérica como lo son Argentina, Colombia, Brasil, México, quienes han implementado políticas penales de manera uniforme respecto a los delitos informáticos, con la firma de este importante acuerdo, la legislación sobre ciberdelincuencia permite flexibilizar determinados mecanismos de obtención de pruebas, en ese sentido se omite la solicitud de autorización judicial para acceder a los datos de los proveedores de comunicaciones, ello sin afectar la privacidad personal, sino más bien siguiendo un protocolo. Para la imputación del delito a los sujetos activos de la ilícita actividad.

Problemática y Contexto social: La ciberdelincuencia está en constante aumento, el Phishing es la modalidad más usada por los delincuentes informáticos

para obtener provecho económico, la comisión de estos delitos afecta absolutamente a todos los usuarios de las entidades financieras, dado que es cotidiano realizar transacciones financieras a través de aplicativos tecnológicos. Según Luján (2023), Perú se encuentra ubicado en tercer lugar de Sudamérica con mayor cifra de casos de phishing, tal y como señala en su informe (p.1). Esto es evidente en las cifras de incidencia delictiva relacionadas con los delitos de phishing. De igual manera Astete (2023) señala “La DIVINDAT, en lo que va del 2023 se han registrado 1,588 denuncias por delitos informáticos” (p.2). Razón por la cual se debe de precisar que, el marco normativo de delitos informáticos N.º 30096 y su reforma a través de la Ley 30171 no contemplan el surgimiento del phishing, situación que pone en riesgo a la ciudadanía al no estar reguladas estas modalidades ilícitas en el actual marco legal peruano. Por ello se debe de realizar la incorporación de esta tipología contribuyendo a la efectividad del actual marco legal establecido en la Ley N° 30096. Para disminuir las cifras de estos delitos, que generan perjuicio a la ciudadanía.

Por estas consideraciones, se formula el **problema de investigación**, como Problema General: ¿Cuál es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024?; asimismo, el problema específico 1. planteado es, ¿Desde el aspecto normativo legal cuál es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia?, problema específico 2 ¿Desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024? O.E. 3 Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

La Justificación Teórica de la tesis consiste en la búsqueda de información de fuentes confiables que permitan ahondar en referencia al tema elegido, en ese sentido se realizará el análisis jurídico respecto al phishing. en esa línea de ideas tenemos al Convenio de Budapest, el mismo que sienta los cimientos para otorgar protección jurídica a las personas, a través del fortalecimiento de lazos a nivel internacional, de esta manera muchos de los países partes en este importante convenio buscan uniformar procesos para delimitar los procesos en el caso de Delitos informáticos. Con respecto a la **Justificación metodológica**, Para obtener los objetivos de la

presente tesis, se realizó un proceso de sistematización, siguiendo el enfoque cualitativo en ese sentido se siguió las técnicas de la investigación. Las mismas que permitieron obtener resultados favorables toda vez que con ese proceso se recuperó información necesaria para poder efectuar un estudio a profundidad permitiendo obtener resultados óptimos, toda vez que las fuentes de información han permitido que se sistematice información relevante a nivel nacional e internacional. Para finalizar, **la Justificación Práctica**, se encuentra encaminada a la búsqueda de la tipificación de esta nueva modalidad delictiva, tal y como se hace mención en líneas precedentes nuestro actual marco normativo legal, no consagra la figura antijurídica del phishing informático, situación que hace imposible la existencia de una tipificación de estos ilícitos penales, que como lo indique generan una afectación netamente patrimonial, dado que el sujeto activo de la conducta atípica busca lesionar bienes jurídicos.

La contribución de la actual tesis, está orientada a penalizar las modalidades delictivas de phishing en nuestro país, en tal aspecto en la actualidad todas las operaciones financieras se desarrollan a través de aplicativos tecnológicos, razón por la cual existe una vulneración a bienes jurídicos que afectan a personas naturales como jurídicas. Por consiguiente, en la ciudad de Lima, estos delitos son los más denunciados y al no existir legislación que consagre estas modalidades delictivas la efectividad de mecanismos para penalizar estas conductas son nulas. Razón por la cual urge penalizar estos delitos, por otro lado, el objetivo general de la tesis es: analizar cuál es la actualidad jurídica del phishing en el sistema penal peruano para la lucha contra la ciberdelincuencia, 2024, como O.E.1. Analizar cuál es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024, O.E.2 Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024, O.E. 3 Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

Finalmente, como **supuesto general**, posibilidad de incorporar el phishing en el Sistema Penal Peruano es sumamente necesaria debido que, la falta de disposiciones legales específicas dificulta la persecución efectiva de los responsables de daños

ambientales significativos. Respecto al supuesto específico uno, La actualidad jurídica phishing en el S.P.P, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales e invita a interpretaciones descontextualizadas y el supuesto específico dos, La actualidad jurídica phishing en el S.P.P, desde el aspecto doctrinario en el S.P.P, es obsoleto y desactualizada.

Respecto al **marco conceptual** el delito *de phishing informático* es una modalidad novedosa respecto a otros delitos penales, ya que la comisión de estos delitos tiene lugar en el ámbito de la tecnología, es decir, a través de internet. Sin embargo, debido a la incidencia de estos delitos, se han llevado a cabo investigaciones internacionales y nacionales en busca de la penalización del delito de phishing. A nivel **Nacional** tenemos a Mengoa (2021), el autor señala que en efecto existe una falta de tipificación para poder encuadrar esta modalidad delictiva de phishing, situación que pone en riesgo la disminución de estos ilícitos penales (p.33). Por otra parte, Paredes (2017) el autor señala que al existir vacíos legales respecto al phishing los delitos se siguen cometiendo generando perjuicio a la ciudadanía. Situación que debe de ser revertida con una correcta imputación de este delito (p.248) Adicional a ello, Mori (2019), sostiene la existencia de falta de capacitación a los operadores de justicia, situación que no permite que se administre justicia de manera eficiente, debemos de tomar en consideración que muchos de los jueces desconocen aspectos informáticos imposibilitando que se actúe con la rigidez que merecen estos ilícitos penales. (p.72).

En ese sentido, Hanco (2018), sostiene que no existe una conexión entre el delito cometido y la sanción que los criminales reciben, de esta manera se aprecia que en efecto al no existir una norma expresa que sancione el phishing, existe inimputabilidad de estos ilícitos. (p.149) Por ello, Espinoza (2017), en su investigación tuvo por objetivo analizar la eficacia de los delitos de phishing, el autor llega a la conclusión que lastimosamente no existe una sanción idónea en el caso de estos ilícitos penales toda vez que existe poco conocimiento del surgimiento de este delito, situación que pone en grave peligro a los ciudadanos. A decir de Fuentes (2021), quien refiere que se debe sancionar los delitos del phishing, como una nueva modalidad delictiva, dado que actualmente hay una imposibilidad de imputabilidad de ilícitos, los mismos que causan inseguridad jurídica. En ese sentido, García (2019) describe que deben de existir garantías para prevenir y erradicar estos delitos en ese

sentido se debe de otorgar mayor rigurosidad en los procesos de transacciones u operaciones a través del campo tecnológico.

Acosta y García (2020) plantean que existe cierta impunidad en la comisión de delito de phishing toda vez que imputar estos delitos implica que el Estado tenga normas dinámicas para delimitar estos ilícitos penales consiguiendo castigar al sujeto activo que realiza la actividad ilícita. Mayer y Oliver (2018) en su artículo de revisión de literatura sostiene que en efecto existen ciertos vacíos legales para determinar la penalización del phishing, dado que no se contempla el phishing como una modalidad en el ordenamiento jurídico peruano. De igual forma, Salvi (2019), señala que en la norma penal no existe la tipificación de este ilícito penal, situación que refiere que se tiene que añadir una norma que proteja estos nuevos tipo penales. Por ello, es adecuado afirmar que no existe una tipificación de estas nuevas tipologías criminales, en tal sentido pese a tener la ley de delitos informáticos al no consagrarse estos ilícitos existe una flagrante deficiencia legal respecto a imputar dichos delitos.

A nivel **internacional**, tenemos a Matute (2017), quien señala que, debido al aumento del phishing, Ecuador se ha ido adaptando a las nuevas conductas delictivas que se realizan en el espacio digital (p.125). Esta situación pone en manifiesto los avances del delito de phishing, situación que afectan a los usuarios de cualquier entidad financiera, para hacerle frente a la comisión de estos delitos, el país vecino ha tenido que fortalecer medidas para disminuir el delito de phishing informático. En esa misma línea de investigación tenemos a Herrero (2021), en su investigación refiere que el Phishing es un delito nuevo que merece una tipificación idónea para erradicar la alta incidencia de estos delitos. En tal sentido es adecuado afirmar que estos delitos al desarrollarse en la esfera digital, la imputación para la obtención de las pruebas digitales es muy difícil de identificar a los agentes. Situación que debe de ser revertida con la tipificación en nuestro ordenamiento jurídico. En ese sentido, Terán (2016), concluyo en su investigación que se debe de añadir la figura jurídica de este delito dado que con una regulación idónea se protegerá a los usuarios y la incidencia de este delito disminuiría (p.108). Definitivamente al regular este nuevo delito, se podrá realizar un encuadramiento correcto a la hora de perseguir este delito.

Adicional a ello, Zapata (2019) señala que existe ineficacia normativa respecto al Phishing ya que no hay un postulado general para la tipificación de este ilícito penal,

de esta manera el autor nos da un panorama sobre estos delitos Señalando que las normas para hacerle frente al phishing son inadecuadas e insuficientes debido al carácter temporal de la norma, aunado a ello el poco conocimiento tecnológico contribuye a la realización de estos ilícitos penales. A decir de Flores (2017), las personas que son víctimas de los delitos de phishing creen que los mensajes y llamadas son de una entidad financiera, situación que pone en riesgo al consumidor quien de buena fe accede a un link que es aparentemente enviado por una entidad real sin embargo esta fue previamente suplantada para obtener información relevante para obtener algún provecho económico. (p.43).

Otra exploración **internacional** es la realizada por Sowmya et al (2023), en su artículo nos señala la existencia de vulneración de las plataformas, para darle veracidad a la que ha sido previamente clonada para obtener algún provecho económico que causara perjuicio al sujeto pasivo del delito de phishing. Añadiendo a ello, Shoaib (2023), señala que el delito de phishing informático causa perjuicio a todas las personas que utilizan las plataformas digitales. Ello se debe principalmente a que los usuarios desconocen cómo manejar de manera correcta el uso de las plataformas digitales y son sorprendidos con mensajes, llamadas telefónicas o link vía mensaje de texto que los inducen al error con mensajes que señalan que han ganado algún premio, sin embargo, ese link solo busca obtener información para ser utilizada en la comisión de estos delitos. Para Tian et al (2023) en su investigación sobre el Phishing refiere que este delito se desarrolla de manera colectiva es decir hay una pluralidad de participantes y la afectación vulnera varios bienes jurídicos en su mayoría prima la obtención del factor económico. A decir de Gupta & Bansal (2023) la comisión de estos delitos como el phishing consiste en inducir al error al usuario quien cree que accediendo a un link de búsqueda a una entidad se encuentra en un lugar seguro sin embargo es falso lo que permite convertirse en una víctima más de la delincuencia informática. En su artículo sobre el phishing, Opara et al (2023) señalan que este delito tiene una alta incidencia y, por tanto, merece un tratamiento jurídico adecuado para erradicar dicha conducta con relevancia penal. De lo expuesto por la autora, se desprende que existen lagunas legales a nivel internacional en la determinación de los autores del phishing informático, y ello se debe al espacio en el que se produce. Esta situación debe revertirse con una regulación integral y la previsión de mecanismos para identificar a los sujetos activos que realizan actividades

contrarias a la ley.

Tenemos como **Bases Teóricas** al Convenio de Budapest el mismo que tiene por finalidad la de otorgar seguridad jurídica a las personas, creando nuevos estándares de criminalidad. En ese sentido como es de conocimiento general, las nuevas tecnologías han traído desarrollo, pero a su vez tienen situaciones que han generado perjuicio, ya que la criminalidad informática está en constante desarrollo debido al poco conocimiento de esta importante herramienta. Cabrera (2017) señala que la Teoría constitucionalista, respecto al delito informático, se encuentra asentada básicamente en la protección constitucional de bienes jurídicos que se encuentran protegidos por la constitución política del estado, es decir que la lesión que se cause debe estar orientada a los derechos establecidos en nuestra carta magna. Téllez Valdés (2008), sostiene que la Teoría clásica, está orientada a identificar las acciones que realice el sujeto activo en la comisión del delito informático de phishing el mismo que debe de ser es típica antijurídica y culpable, si no cumplan con estos elementos no pueden ser considerados delito informático.

Cabrera (2017) señala que *la teoría constitucionalista*, respecto al delito informático, se encuentra asentada básicamente en la protección constitucional de bienes jurídicos que se encuentran protegidos por la constitución política del estado. Finalmente, la subcategoría que es *derecho comparado* en donde el autor matute (2017) señala que, debido al aumento de phishing. Ecuador se ha ido adaptando a las nuevas conductas delictivas que se realizan en el espacio digital (p, 125).

La Teoría del patrimonio-personalidad, hace referencia a los bienes patrimoniales presentes y futuros por ende merecen protección legal por parte de los operadores de justicia, en tal sentido frente a una afectación patrimonial estado tiene la obligación legal de perseguir el delito. Para Gamio (2018) el patrimonio está orientado a obtener un fin económico ya que el patrimonio está constituido por bienes, derechos y acciones que se desarrolla de manera personal. En los delitos informáticos La teoría de los Bienes jurídicos afectados son el patrimonio toda vez que el sujeto activo busca lucrar con el desconocimiento de las personas que accede a las plataformas digitales previamente suplantadas por los cibercriminales, razón por la cual corresponde al estado proteger estos Bienes jurídicos los mismos que son supraindividuales.

En nuestro ordenamiento jurídico, urge la realización de una lucha frontal contra la ciberdelincuencia, con el objetivo de poner en salvaguarda los derechos fundamentales, sancionando y erradicando a los ciberdelincuentes, en ese sentido se debe de ser más dinámicos respecto a nuevos ilícitos que lastimosamente no se encuentra establecido en la norma legal actual. Conceptualmente el significado de delitos informáticos; hace referencia al ilícito que se desarrolla en esa esfera tecnológica son, en ese sentido el injusto se lleva a cabo mediante la acción típica, antijurídica o culpable. Dado que el agente tiene pleno conocimiento que su conducta busca lesionar y o afectar el patrimonio de los usuarios que acceden a plataforma digital. El phishing, consiste en inducir al ardid a las personas para que se pueda sustraer su información personal con el objetivo de sacar provecho económico. Este delito tiene dos fases o modalidades: la primera consiste en fraguar la identidad de alguna entidad bancaria y la segunda a través de links, correos o llamadas telefónicas. En el delito de phishing, el sujeto activo busca extraer información privada como lo son los usuarios y contraseñas personales para más adelante tener un beneficio económico, en relación a esto, García (2020), señala que la utilización de nuevos dispositivos tecnológicos contribuye a que estos ataques por los delincuentes tecnológicos. Desde el mismo modo, López (2021), nos refiere que esa técnica se da a través de una llamada telefónica que busca concretar el ilícito penal haciendo creer a la víctima que se trata de una llamada real. En ese sentido comparto la postura de Hidalgo y Solano (2021) quien señala que nuestro actual marco normativo no posee una norma con estas nuevas modalidades antes descritas situación que pone en riesgo las transacciones financieras. Ortiz (2019) señala que estos delitos se perpetran en la esfera tecnológica, y corresponde a los estados buscar la reducción de los índices de criminalidad, empleando para ello los mecanismos jurídicos necesarios para imputar responsabilidad penal a las entidades financieras. Por otro lado, Pardo (2018) concluye que existe deficiencia en el actual marco normativo y tal y como lo hemos dilucidado líneas más arriba en efecto afecta una norma deficiente que dificulta una sanción efectiva de aquellos delitos contra el patrimonio que se desarrollan en el espacio digital. Por todo lo señalado considero que se debe penalizar las nuevas modalidades de estos ilícitos penales. De esta manera se sancionarán estos delitos que tienen alta incidencia en nuestro país, en ese extremo, a la hora de perseguir el delito se deben de imputar correctamente estos nuevos tipos penales, de esta manera se podrá otorgar de protección en el ciberespacio que todas las

operaciones financieras, se desarrollen con la seguridad necesaria.

A continuación, se trabajará **el marco Jurídico comparado**. En Chile existe una regulación penal de delitos informáticos a través de La ley 21459 el país vecino les hace frente a estos ilícitos penales, de esta manera se describe los tipos penales que tendrán relevancia jurídica para la búsqueda de sanción penal. Si bien es cierto en la legislación antes descrita no se tipifica el phishing informático como tal, el artículo 06 de la citada ley hace mención a la falsificación informática una figura que sanciona una conducta reprochable que busca generar perjuicio económico. En Brasil, Los delitos informáticos se encuentran regulados a través de la Ley núm. 12737, que sanciona los ilícitos informáticos, con el objetivo de perseguir el delito para sancionarlo y erradicarlo, en tal sentido en la legislación brasileña se sanciona a las personas que vulneren los datos privados como las contraseñas obtenidas de manera ilegal. En México, el Código Penal Federal de México, sanciona los delitos informáticos con el objetivo de salvaguardar los bienes jurídicos de los ciudadanos mexicanos, esta ley de delitos informáticos, establece que comete delito informático, la persona que dolosamente y sin derecho, use o entre a una base de datos con el objetivo de generar algún beneficio en perjuicio de otro. En Colombia, la ley de delitos informáticos se encuentra regulado a través de la Ley 1273, el artículo 269G hace referencia a la suplantación de sitios web sanciona todo tipo de medio para inducir al error a las personas. De esta manera se sanciona los actos preparatorios y posteriores para causar una lesión para obtener algún provecho económico.

II. METODOLOGÍA

En el presente trabajo se desarrolló el **tipo de estudio, enfoque y diseño de investigación**. En ese sentido el *enfoque cualitativo* en que se basa la presente investigación. Para Fernández (2014) el enfoque cualitativo busca indagar y sistematizar la información desde la perspectiva de los participantes. Esta tesis fue de *tipo básico*. Según Álvarez (2020), señala que este tipo de investigación se enfoca en la adquisición de la información nueva con el objetivo de incrementar el existente. En concordancia con lo señalado por el autor el *tipo de investigación básica* nos permite a través de la búsqueda de la información y los saberes previos, obtener una información con relevancia jurídica para abordar un tema de manera idónea. Respecto al *diseño de investigación* de investigación consideramos que la teoría fundamentada: nos permite tener una conceptualización de las teorías cumpliendo todos los estándares de la investigación es decir mediante los datos obtenidos recabados en la búsqueda de la información nos permitió comparar aspectos para fundamentar la información (De la Espriela y Gómez, 2022, p.1). En este sentido, concuerdo con lo que refieren los autores toda vez que esta teoría nos permite tener idea propia dinamizando el proceso de investigación toda vez que mediante este diseño de investigación los resultados serán los deseados por el investigador partiendo desde las teorías recabadas en los antecedentes de la investigación.

Sucesivamente, se menciona la definición de **las categorías y subcategorías** establecidas en la presente exploración, por ende, la primera categoría es el phishing donde el autor Cárdenas y Mejía (2021) determina que el phishing es un tipo de fraude lo cual consiste en enviar mensajes de texto de páginas falsas, suplantando instituciones bancarias, a fin de lograr información, como claves de acceso de los usuarios. En compilación, se observa que las subcategorías ya definidas son clase de fraudes informáticos y por ello su magnitud al conocerlas adecuadamente. Finalmente, la subcategoría sistema penal peruano en donde el autor Ortiz (2019) señala que estos delitos se perpetran en la esfera tecnológica, y corresponde a los estados buscar la reducción de los índices de criminalidad, empleando para ello los mecanismos jurídicos necesarios para imputar responsabilidad penal a las entidades financieras.

continuamente, su definición de *las subcategorías* establecidas en la investigación, y como la 1ra subcategoría tenemos a *normativa legal* donde la legislación sobre delitos informáticos N° 30096 y su alteración a través de la ley 30171 no contempla el surgimiento del phishing, situación que pone en riesgo a la ciudadanía al no estar reguladas estas modalidades ilícitas en el marco legal. La siguiente subcategoría denominada *la doctrina* donde

Tabla 01

Tabla de categorización

Categoría de estudio	Definición conceptual	Sub categorías	indicadores
Phishing	Según Herrero (2021), el Phishing es un delito nuevo que merece una tipificación idónea para erradicar la alta incidencia de estos delitos.	Normativa legal	-sistemas -legales -penal -interpretacion
		Doctrina	
Sistema penal peruano	Para Ortiz (2019) señala que estos delitos se perpetran en la esfera tecnológica, y corresponde a los estados buscar la reducción de los índices de criminalidad, empleando para ello los mecanismos jurídicos necesarios para imputar responsabilidad penal a las entidades financieras.	Derecho comparado	-sistemas -legales -penal -interpretación

Ante la presente situación los **participantes**, para Martínez et. al. (2021) vienen siendo parte vital en una investigación. Toda vez que esos sujetos permiten el acercamiento a las cualidades del investigador. Por ello se hace necesario señalar de manera cercana las cualidades del entrevistado o los elementos que van a intervenir en él. También se plantea *el escenario de estudio* se fue realizado en la ciudad de Lima, realizando la aplicación de las entrevistas; teniendo como apoyo a abogados especialistas.

Tabla 02:*Participantes*

Entrevistados	grado académico	experiencia laboral	años de experiencia
Elbert Guerra Peláez	Doctor	Colegiado y especialista en derecho penal.	20
Judith Obregón Isidro	Magister	Abogado especialista en derecho penal y laboral	10
Guillermo Lleren Perez	Abogado	Abogado	02
Sandra Franchezca Vilchez Alvarado	Abogada	Abogada	02
Mayra Manzanilla Torres	Abogado	Abogado	04
Gustavo Castillo Martínez	Magister	Abogado especialista en lo civil	05
Uber Dante Gómez Basilio	Abogado	Abogado especialista en lo administrativo	10

Mencionando a las **técnicas e instrumentos de investigación** de la tesis. Se va a trabajar en un primer momento con la *técnica de la entrevista*. En donde, Vásquez, et al. (2023), hace mención que la recopilación de datos, que se realiza es para reunir información, la cual será pieza importante para llegar a verificar supuestos planteados en una investigación. Ahora, desarrollaremos *los instrumentos de investigación*. En ese sentido, utilizaremos los instrumentos de G.A. normativo legal, G. A. doctrinario y la G.A. de derecho comparado.

En cuanto al *rigor científico*, se subraya la escrupulosidad empleada conforme a las directrices establecidas por la normativa académica vigente, lo cual asegura la pertinencia y fiabilidad requeridas. Asimismo, he seguido los lineamientos institucionales de nuestra alma mater para recabar la información necesaria, la cual guarda una estrecha relación con el enfoque y diseño de mi tesis, dando como resultado la creación de una investigación sólida, fundamentada en premisas veraces y dirigida hacia la formulación de conclusiones legítimas.

Tabla 03:*Validez de Instrumento: Guía de Entrevista*

Validador	Cargo	Institución
Elbert Augusto Guerra Peláez	Abogado y Gerente.	Estudio jurídico Guerra Peláez(GUPELSAC).
Judith Beatriz Obregón Isidro	Abogada	Estudio jurídico Obregón Isidro
Mayra Meribeth Manzanilla Torres	Abogada	Estudio Jurídico Manzanilla y asociados.

Tabla 04:*Validez de Instrumento: documento de análisis normativo*

Validador	Cargo	Institución
Elbert Augusto Guerra Peláez	Abogado y Gerente.	Estudio jurídico Guerra Peláez(GUPELSAC).
Judith Beatriz Obregón Isidro	Abogada	Estudio jurídico Obregón Isidro
Mayra Meribeth Manzanilla Torres	Abogada	Estudio Jurídico Manzanilla y asociados.

Tabla 05:*Validez de Instrumento: documento de análisis doctrinario*

Validador	Cargo	Institución
Elbert Augusto Guerra Peláez	Abogado y Gerente.	Estudio jurídico Guerra Peláez(GUPELSAC).
Judith Beatriz Obregón Isidro	Abogada	Estudio jurídico Obregón Isidro
Mayra Meribeth Manzanilla Torres	Abogada	Estudio Jurídico Manzanilla y asociados.

Tabla 06:*Validez de Instrumento: documento de análisis de derecho comparado*

Validador	Cargo	Institución
Elbert Augusto Guerra Peláez	Abogado y Gerente.	Estudio jurídico Guerra Peláez(GUPELSAC).

Judith Beatriz Obregón Isidro	Abogada	Estudio jurídico Obregón Isidro
Mayra Meribeth Manzanilla Torres	Abogada	Estudio Jurídico Manzanilla y asociados.

En desarrollo de la presente investigación se viene utilizando diversos **métodos de análisis de datos**, siendo los siguiente: el método inductivo este nos permitió analizar la información desde un aspecto específico hasta llegar a algo general, situación que nos permitió tener una visión más clara respecto al tema planteado A decir de Prieto (2017) indica que: este método nos permitió desde un hecho concreto construir al recopilar la información hasta conseguir fundamentos teóricos En consecuencia también se utilizó el método Hermenéutico: toda vez que en el actual ordenamiento jurídico existen vacíos legales de esta manera se buscara minimizar dichas deficiencias. En este sentido el autor Ortiz (2015) señala que este método nos permite comprender los datos recabados en el proceso de investigación (p.16). De la misma manera el método Sintético: Después de analizar los resultados se sistematizarán, haciendo un resumen sobre la información previamente obtenida. A decir de Rus (2021) este método resume todos los aspectos más relevantes de la investigación.

En cuanto a los **aspectos éticos**, este estudio se llevó a cabo siguiendo principios axiológicos y evitando influencias sesgadas o parciales sobre el problema de investigación. Además, se condujo la investigación científica de acuerdo con el método científico, adoptando un enfoque cualitativo conforme al esquema establecido por la universidad y las directrices del asesor teórico y metodológico. Se emplearon técnicas de recolección de datos cualitativos como entrevistas y análisis documental para contextualizar adecuadamente el problema de investigación dentro de los procedimientos administrativos pertinentes. También se garantizó el respeto al espacio de los entrevistados, permitiendo su retiro en cualquier momento durante la entrevista. Asimismo, se observaron las normas de propiedad intelectual al citar correctamente las fuentes bibliográficas utilizadas según el estilo APA.

III. RESULTADOS

Subcategoría Normativa legal

Continuando, se procederá a explicar y detalladamente los hallazgos de estudio, utilizando el método de **entrevista** y optando como referencia los hallazgos están asociados con el objetivo específico 1, que consiste en explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024. Por lo tanto, se han obtenido los siguientes resultados.

Para responder al objetivo específico 1 se realizaron dos preguntas, la primera de ellas consistió en determinar si considera que la actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales, es por ello sé que obtuvo como resultado que los entrevistados Vilchez, Gómez y Guerra, señalaron que existen vacíos legales respecto a la figura delictiva de phishing informático, por ende, señalan que no hay una correcta imputación de esta figura delictiva; mientras que LLeren, Manzanilla, Castillo, nos refieren que el actual marco normativo legal no contempla una regulación idónea respecto a este tipo de delitos, toda vez que la norma legal vigente solo contempla al fraude informático. Opinión contraria la conseguimos por parte de Obregón, quien refiere que la ley de delitos informáticos con la nueva modificación contempla esta figura delictiva de Phishing. Como vemos y llegar a la conclusión que en su gran cantidad de los entrevistados seis de siete de señalan que la actualidad jurídica del Phishing presenta vacíos legales, pese a la modificación de la ley de delitos informáticos.

En cuanto a la segunda pregunta que consistió en desde su experiencia, cree Ud. Que actualidad jurídica phishing en el S.P.P, desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas en Se han obtenido los siguientes resultados producto de las entrevistas realizadas a los especialistas en Derecho Penal. En ese sentido Vilchez y Guerra señalaron que no existe un tratamiento jurídico idóneo por ello a la hora de imputar este tipo de delitos solo se realiza de acuerdo a Lo establecido en la ley de delitos informáticos como fraude. El entrevistado LLeren va más allá y señala que la ley de delitos informáticos pese a una reciente modificatoria muestra una descontextualización y ello se debe a

la inexistencia de una interpretación normativa. Gómez, Castillo y Manzanilla señalaron que existe una mala interpretación de la norma causando vacíos legales. Una opinión contraria la vemos en Obregón quien señala que con la nueva modificación de la ley de delitos informáticos se ha superado la carencia de existencia de una norma que describa este tipo penal. Como podemos analizar y a manera de concluir la mayoría de los entrevistados para ser exactos seis de siete de ellos mencionan que existen vacíos legales respecto al actual marco normativo.

En este momento, se llevará a cabo la exposición y explicación de los resultados de estudio empleando **la técnica del análisis documental**, especialmente enfocado en el análisis normativo legal. Para esto, se ha optado por iniciar con los resultados obtenidos y vinculados al O.E. 1 donde se busca explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el S.P.P, para la lucha contra la ciberdelincuencia, 2024, se tiene a partir de la revisión de lo establecido en la ley de delitos informáticos lo siguiente: informáticos lo siguiente:

Tabla 7

Análisis normativo legal

nombre del articulo	Articulo citado	Interpretación	Calificación/ Actualizado desactualizado
Fraude informático Art. 8	Quien intencionalmente y de manera ilegítima busca obtener una ganancia ilícita para sí mismo o para otro, causando perjuicio a terceros mediante el diseño, inserción, modificación, eliminación, clonación de datos informáticos (...).	De acuerdo al artículo citado, se observa la definición expresa del fraude informático mas no se menciona al phishing, por lo que se entiende que no existe una regulación actual al respecto.	<i>desactualizado</i>
Decreto legislativo 1614 que modifica Ley 30096 de delitos informáticos Art. 8	Quien intencionalmente y de manera ilegítima busca obtener un beneficio indebido para sí mismo o para otra persona, causando daño a un tercero mediante el diseño, introducción, alteración, borrado, supresión, (...)	El articulo señalado no describe la figura delictiva del phishing informático, por ende, se requiere una actualización de la norma.	<i>desactualizado</i>

<p>convenio sobre ciberdelincuencia de Budapest art. 8</p>	<p>Las partes adoptarán las disposiciones legislativas o las que estimen pertinentes para clasificar como delitos en su jurisdicción nacional los actos ilícitos que resulten en pérdidas económicas (...).</p>	<p>Este convenio pactado menciona de manera general para combatir la ciberdelincuencia y mas no hace mención sobre el phishing.</p>	<p><i>desactualizado</i></p>
<p>Ley de Delitos Informáticos Art. 1</p>	<p>El propósito de esta ley es prevenir y penalizar las acciones ilegales que impactan los sistemas, datos informáticos y otros bienes jurídicos de importancia penal, realizadas utilizando tecnologías de la información o comunicación, con el objetivo de combatir eficazmente el crimen cibernético.</p>	<p>La ley mencionada abarca la ley de protección de datos personales y mas no hace mención al phishing</p>	<p>desactualizada</p>
<p>Artículo 2.- Acceso ilícito</p>	<p>Quien acceda sin autorización a la totalidad o parte de un sistema informático, vulnerando las medidas de seguridad establecidas para evitarlo, será castigado con una pena de prisión no menor de uno ni mayor de cuatro años y una multa de treinta a noventa días. Igual pena se aplicará a quien acceda a un sistema informático excediendo los límites de la autorización otorgada.</p>	<p>El citado artículo no hace mención ninguna sobre la modalidad del phishing y por lo tanto no hay una adecuada mención actual.</p>	<p><i>desactualizada</i></p>
<p>Artículo 4. Atentado a la integridad de sistemas informáticos</p>	<p>Quien de manera deliberada e ilegítima desactive total o parcialmente un sistema informático, impida el acceso al mismo, dificulte o impida su funcionamiento o la prestación de sus servicios, será sancionado con una pena de prisión no menor de tres ni mayor de seis años, además de una multa de ochenta a ciento veinte días.</p>	<p>Dentro del artículo n hay una mención directa sobre el phishing y es por ello que existe un vacío que debería ser mencionada para su correcta interpretación.</p>	<p><i>desactualizada</i></p>

Se realizará el comentario de los resultados de la presente investigación expuestos al *O. E. 1* que consiste en comentar desde el aspecto normativo legal cuál es la actualidad jurídica del phishing en el S.P.P., para la lucha contra la ciberdelincuencia, 2024, por ello, de la revisión de los 7 articulados comprendidos en la ley de delitos informáticos, ninguno de ellos plantea algo favorable, sobre los actos preparatorios que tiene la figura delictiva del phishing como nueva modalidad delictiva, razón por la cual urge una legislación adecuada que contemple esta figura con el objetivo de disminuir los altos índices de criminalidad informática.

Tabla 8

Resultados del objetivo específico 1

Objetivo específico 1	Técnica	Actualizado	desactualizado
Explicar desde el aspecto normativo legal cuál es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.	Entrevista	Un entrevistado refiere que el actual marco normativo, al tener una modificatoria contempla la figura delictiva del Phishing informático por ende no existe vacío legal ni invita a una descontextualización	Los entrevistados en mayorías sostienen que existen vacíos legales en la ley de delitos informáticos. Seis de siete entrevistados refiere que el sistema penal peruano invita a interpretaciones descontextualizadas respecto al phishing.
	Análisis documental	No existe información que señale la imputación de fraude informático	De la revisión de los 03 articulados comprendidos en la ley de delitos informáticos, ninguno de ellos plantea la figura delictiva de Phishing.

Basándose en la información recopilada mediante las entrevistas y el análisis documental, se tiene como **resultado del objetivo específico 1**, revela que la mayoría de los entrevistados, es decir 6 de 7 entrevistados, (primera y segunda pregunta respectivamente), junto con los hallazgos del análisis documental, tenemos como resultados que los articulados expuestos que la ley de delitos informáticos no contempla la figura delictiva del phishing informático, razón por la cual urge una modificación a la norma.

Subcategoría Doctrina

Se procederá el esclarecimiento de los resultados de este estudio, utilizando la técnica de la entrevista y tomando como referencia los resultados vinculados al O.E. 2 que consistió en Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el S.P.P., para la lucha contra la ciberdelincuencia, 2024. A partir de ello, se han obtenido los siguientes resultados.

Para responder al O. E. 2 se realizaron dos preguntas, la numero uno de ellas consistió en ¿Ud. considera que La actualidad jurídica phishing en el S.P.P., desde el aspecto doctrinario, para la lucha contra la ciberdelincuencia, 2024. es obsoleto?, se obtuvo como resultados los siguientes. En este caso, todos los participantes en la entrevista dijeron que se descubrió que la mayoría de los participantes (Vilchez, Guerra, LLeren, Manzanilla, Gómez y Obregón) señalaron que doctrinariamente la figura delictiva del Phishing en nuestro país es nula, razón por la cual para estudiar este tipo de modalidad o tipo se debe de recurrir a legislación internacional, es decir que para abordar esta información se debe de estudiar doctrinariamente consultando fuente internacional. En ese sentido es uniforme por parte de los entrevistados al señalar que existe un poco aproximación de delitos informáticos.

Asimismo, la segunda pregunta de investigación que consiste en desde su experiencia, Ud. ¿Cree La actualidad jurídica phishing en el S.P.P. , desde el aspecto doctrinario en el sistema penal peruano es desactualizada? En ese sentido Vilchez, Guerra, LLeren, Manzanilla, Gómez, Castillo y Obregón refirieron de manera uniforme que Doctrinariamente no hay mucha información respecto al Phishing situación que pone en riesgo futuras imputaciones a sujetos activos que realicen actividades ilícitas.

Procederemos a presentar y a detallar los resultados de esta investigación empleando el enfoque del análisis doctrinario, específicamente en lo referente al análisis normativo legal. En este contexto, nos centraremos inicialmente en los resultados relacionados con el O.E. 2, el cual aborda la explicación doctrinal sobre la situación jurídica actual del phishing en el marco del sistema penal peruano, en el contexto de la lucha contra la ciberdelincuencia en el año 2024.

Tabla 9*Normativa Doctrinaria*

Autor, Año, página	Cita textual	Interpretación	Califi cació n
Valle Matute Juan(201 7, p.125)	Señala que, debido al aumento del fraude, Ecuador se ha ido adaptando a las nuevas conductas delictivas que se realizan en el espacio digital Esta situación pone en manifiesto los avances del delito de phishing como fraude.	El autor señala que existe una novísima modalidad delictiva que surge en la esfera de la era tecnológica, razón por la cual la actualización de normas legales permitió hacerle frente a esa nueva modalidad delictiva.	Desactualizada
Herrero, (2021, p.75)	Herrero (2021), en su investigación refiere que el fraude es un delito nuevo que merece una tipificación idónea para erradicar la alta incidencia de estos delitos.	En tal sentido es adecuado afirmar que estos delitos al desarrollarse en la esfera digital, la imputación para la obtención de las pruebas digitales es muy difícil de identificar a los sujetos activos. Situación que debe de ser revertida con la tipificación en nuestro ordenamiento jurídico	Desactualizada
Zapata, (2019, p.30)	señala que existe ineficacia normativa respecto al fraude ya que no hay un postulado general para la tipificación de este ilícito penal.	De esta manera el autor nos da un panorama sobre estos delitos Señalando que las normas para hacerle frente al fraude son inadecuadas e insuficientes debido al carácter temporal de la norma, aunado a ello el poco conocimiento tecnológico contribuye a la realización de estos ilícitos penales	Desactualizada
Flores. (2017, p.43)	Las personas que son víctimas de los delitos de fraude creen que los mensajes y llamadas son de una entidad financiera, situación que pone en riesgo al consumidor quien de buena fe accede a un link que es aparentemente enviado por una entidad real sin embargo esta fue previamente suplantada para obtener información relevante para obtener algún provecho económico. (p.43)	El fraude, hace referencia a los medios por los cuales se vale el sujeto activo para la comisión de estos delitos, en tal sentido el autor nos señala una serie de actos preparatorios para cometer este delito informático.	Desactualizada
Paredes (2017, p.248)	El autor señala que al existir vacíos legales respecto al fraude los delitos se siguen cometiendo generando perjuicio a la ciudadanía. Situación que debe de ser revertida con una correcta imputación de este delito.	A decir del autor estos delitos tienen incidencia dado que no existe legislación uniforme para encuadrar estos delitos.	Actualizada

Cabrera (2017, p.43)	Cabrera (2017) señala que la Teoría constitucionalista, respecto al delito informático, se encuentra asentada básicamente en la protección constitucional de bienes jurídicos que se encuentran protegidos por la constitución política del estado, es decir que la lesión que se cause debe estar orientada a los derechos establecidos en nuestra carta magna.	Como es de conocimiento general, las nuevas tecnologías han traído desarrollo, pero a su vez tienen situaciones que han generado perjuicio, ya que la criminalidad informática está en constante desarrollo debido al poco conocimiento de esta importante herramienta	Desactualizada
Téllez Valdés (2008, p.40)	sostiene que la Teoría clásica, está orientada a identificar las acciones que realice el sujeto activo en la comisión del delito informático de fraude el mismo que debe de ser es típica antijurídica y culpable, si no cumplan con estos elementos no pueden ser considerados delito informático.	La teoría clásica nos da una arista elemental respecto a la manera en la que se desarrolla este ilícito penal. Es decir que el actuar del sujeto activo debe de ser antijurídica y culpable.	Desactualizada
Gamio (2018, p.25)	El patrimonio está orientado a obtener un fin económico ya que el patrimonio está constituido por bienes, derechos y acciones que se desarrolla de manera personal. En los delitos informáticos La teoría de los Bienes jurídicos afectados son el patrimonio.	El sujeto activo busca lucrar con el desconocimiento de las personas que accede a las plataformas digitales previamente suplantadas por los cibercriminales, razón por la cual corresponde al estado proteger estos Bienes jurídicos los mismos que son supraindividuales	Desactualizada

CONCLUSIÓN: Se puede apreciar que de los nueve autores comparten los mismos criterios que, tomando como punto de partida el supuesto que se deba de uniformar las normas penales para encuadrar esta nueva figura delictiva que busca sacar provecho es decir lucrar económicamente valiéndose del ardid para cometer ilícitos penales.

Tabla 10

Resultados del objetivo específico 2

Objetivo específico 2	técnico	Desactualizado	Actual
Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en	Entrevista	No existe doctrina nacional que refiera al Phishing en el sistema penal peruano	De manera uniforme, los entrevistados, han llegado a la conclusión que en la actualidad doctrinariamente la figura delictiva de phishing es inexistente

el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.	Análisis doctrinario	No existe información a nivel nacional	Se tiene que recurrir a doctrina internacional, la manera en la que se aborda el tema de delitos informáticos en la modalidad de phishing es nulo en nuestro país, o que genera que los operadores de derecho, no puedan ejercer de manera correcta la imputación de estos delitos situación que pone en riesgo el correcto funcionamiento del sistema penal peruano, a nivel doctrinario en nuestro país si bien es cierto los delitos informáticos tienen alta incidencia criminal, aun no existe una política criminal informática para sancionar a los agentes que realicen estos actos contrarios a nuestro marco normativo
--	----------------------	--	--

En base a lo recogido por las entrevistas y el análisis doctrinario, se tiene como **resultado del objetivo específico 2**, que, por unanimidad de entrevistados, 7 de 7 entrevistados, (3ra y 4ta pregunta respectivamente) esto añadidos a lo señalado por el análisis doctrinario tenemos como resultados , De manera uniforme, los encuestados han llegado a la conclusión que en la actualidad doctrinariamente la figura delictiva de phishing es inexistente.

Subcategoría Derecho Comparado

A continuación, se empleará la técnica de entrevista para presentar y explicar los hallazgos de la investigación actual, tomando como referencia los hallazgos O. E. 3 que consiste en Explicar desde el derecho comparado es la actualidad jurídica del phishing en el S.P.P , para la lucha contra la ciberdelincuencia, 2024. Es así que se han obtenido los siguientes resultados a partir de la quinta pregunta: Ud. ¿considera que La actualidad jurídica phishing en el S.P.P, desde el aspecto del derecho comparado está regulado de manera muy general?

Para responder al O.E.3 se realizó una pregunta, que consistió en Ud. considera que La actualidad jurídica phishing en el S.P. desde el aspecto del derecho comparado está regulado de manera muy general?

También se realiza la presentación y explicación de los resultados de la presente investigación utilizando **la técnica del análisis de derecho comparado** en lo que respecta el análisis de derecho comparado, para ello se ha querido iniciar tomando como referencia los resultados obtenidos y relacionar al O.E. 3 donde se busca

Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema S.P.P, para la lucha contra la ciberdelincuencia, 2024.

Tabla 11

Derecho Comparado

País	Asunto a comparar	Norma legal	Cita	Calificación
Perú	Aplicación de la Ley de delitos informáticos	La Ley de Delitos Informáticos N.º 30096 y su modificación mediante la Ley 30171	La persona que hace uso de la tecnología, con el cual obtiene un bien ilícito para su persona, mediante su penetración, variación, esta será sancionada con una pena de 3 años y no superiores a 8 años o una multa de 60 o 120 días.	Actualizada
Chile	Aplicación y de la ley de delitos informáticos	Ley 21459	Quien, con el propósito de obtener un beneficio económico para sí mismo o para otro, cause daño a otra persona manipulando un sistema informático mediante la introducción, alteración, daño o eliminación de datos informáticos, o cualquier intervención en el funcionamiento de un sistema informático.	Actualizado
Brasil	Ley núm. 12737	Quien viole contraseñas o obtenga datos privados y comerciales sin el consentimiento del titular de la cuenta será sentenciado a una pena de tres meses a dos años de prisión y también se le impondrá una multa.	En Brasil, se castiga a aquel que obtenga datos privados con fines de lucro económico. En Perú, estos delitos son penalizados de manera más estricta, con una pena de prisión no menor de 5 ni mayor de 10 años, además de una multa de 80 a 140 días.	Actualizado
México	Artículo 211 bis 1 Código Penal Federal	Alguien que cambie o haga uso con fines ilícitos una información en sistemas digitales, las cuales están protegidos con mecanismos de protección será sancionado con 6 meses y 2 años de prisión P. L.	En nuestro país, esta conducta se penaliza con una pena de prisión no menor de uno ni mayor de cuatro años y una multa de treinta a noventa días, mientras que en México la pena es de 6 meses a dos años.	Actualizada

Colombia	Ley de delitos Ley 1273	El individuo que interfiera los datos dentro e un S. I. sin una previa orden judicial enfrentara una pena de 36 a 72 meses.	En Colombia, aquel que sin orden judicial vulnere un sistema informático será sancionado con una pena de 36 a 72 meses. En Perú, la pena para esta conducta es de no menos de 1 ni más de 4 años de prisión, acompañada de una multa de 30 a 90 días.	Actualizado
----------	-------------------------	---	---	-------------

Conclusión: Podemos concluir según los artículos mencionados de distintos países este ilícito penal, tiene relevancia jurídica para la búsqueda de sanción penal. Si bien es cierto en la legislación antes descrita no se tipifica el phishing informático como tal, se debe de regular esta nueva figura que sancione esta conducta reprochable que busca generar perjuicio económico.

Tabla 12

Resultados del objetivo específico 3

Objetivo específico 3	Técnica	No vulnerante	Vulnerante
Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024	Entrevista	No existe información	Los entrevistados señalaron que a nivel comparado existe legislación que sirve de base para que el estado pueda sancionar las actividades ilícitas ejecutadas por el agente.
	Análisis de derecho comparado	No existe información	A nivel de derecho comparado se tiene a 4 países, como Chile, Brasil, México y Colombia, tienen legislación referente a los delitos informáticos y la figura delictiva de Phishing.

En base a lo recogido por las entrevistas y el análisis de derecho comparado, se tiene como **resultado del objetivo específico 3**, que todos los entrevistados, esto añadidos a lo señalado por el análisis tenemos como resultados que si bien a nivel internacional es decir mediante el derecho comparado existe información respecto

a los delitos informáticos la actualidad jurídica de nuestro país no contempla dicha figura dentro de nuestra legislación nacional, por ende debemos de corregir esta postura.

3.4. Resultado final de la tesis

Objetivo general

A continuación, se realizará la descripción del resultado final de la tesis tomando como referencia al objetivo general, que consiste en analizar cuál es la actualidad jurídica del phishing en el S.P.P., para la lucha contra la ciberdelincuencia, 2024. En consecuencia, podemos decir que el escenario legal del phishing no se encuentra regulado en nuestra legislación, razón por la cual es desactualizada el actual marco normativo. Primero, *por su falta de regulación normativa*, ya que los artículos comprendidos en la ley de delitos informáticos no contemplan esta figura delictiva del phishing. Segundo, y esto en alusión a lo señalado anteriormente, la ley de delitos informáticos no consagra este tipo de modalidad que es más compleja toda vez que posee actos preparatorios para la comisión de ilícitos penales, causando perjuicio económico a las personas que son víctimas de estos ilícitos toda vez que no se puede imputar este tipo de delitos a los sujetos activos que comenten esta modalidad delictiva. Tercero, *pese a la modificación de la ley de delitos informáticos, esta no ha consolidado un alto a los índices de fraude toda vez que no se imputa de manera idónea a nivel penal. Finalmente, como antes ya lo eh señalado nuestra actualidad jurídica requiere una solución inmediata con la dación de una norma que permita imputar a los sujetos activos de responsabilidad penal en la comisión de phishing informático, ello debido principalmente a los altos índices de criminalidad informática.*

Tabla 13

Resultado final de la tesis

Objetivo general	Desactualizada	Actualizada
------------------	----------------	-------------

Analizar cuál es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

El escenario legal del Phishing informático en nuestro sistema penal peruano es desfavorable y ello se debe a: Primero, por su falta de regulación normativa, ya que los artículos comprendidos en la ley de delitos informáticos no contemplan esta figura delictiva del phishing si no como fraude. Segundo, y esto en alusión a lo señalado anteriormente, la ley de delitos informáticos no consagra este tipo de modalidad que es más compleja toda vez que posee actos preparatorios para la comisión de ilícitos penales, causando perjuicio económico a las personas que son víctimas de estos ilícitos toda vez que no se puede imputar este tipo de delitos a los sujetos activos que comenten esta modalidad delictiva. Tercero, pese a la modificación de la ley de delitos informáticos, esta no ha consolidado un alto a los índices de fraude toda vez que no se imputa de manera idónea a nivel penal. Finalmente, como antes ya lo he señalado nuestra actualidad jurídica requiere una solución inmediata con la dación de una norma que permita imputar a los sujetos activos de responsabilidad penal en la comisión de phishing informático, ello debido principalmente a los altos índices de criminalidad informática.

No existe información

IV. DISCUSIÓN

Iniciaremos el presente apartado realizando una sistematización de la información obtenida a través de la información recabada en las guías de entrevistas, de análisis documental, normativo y comparado. Por ello, en primer lugar, se realizó una discusión con los antecedentes de investigación de esta tesis donde relacionándolo con el *O.E. 1* Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el S.P.P, para la lucha contra la ciberdelincuencia, 2024, como es de conocimiento nuestro ordenamiento jurídico a establecido contemplar la figura delictiva de fraude informático a través de la ley de delitos informáticos Ley 30096, específicamente en su artículo 8, nos menciona al fraude como figura delictiva de persecución de la acción penal, normativamente hablando si bien en nuestro país existe una norma de aseguramiento de sanción a este tipo de delitos informáticos, nuestro ordenamiento jurídico se ha desactualizado respecto a la inclusión de nuevas formas de fraude informático, como lo es el Phishing, al no cumplir nuestros legisladores su rol dinámico respecto a dación de normas, esta figura delictiva cobra relevancia jurídica dado el contexto en el que se desarrolla es decir en el ciberespacio, hablar de fraude es básico en la actualidad dado que no siempre se manipula una página web para robar información de gente incauta que por carecer de conocimiento tecnológico es víctima de ciberdelincuentes y al no existir una norma que consagre otros tipos de delitos informáticos hacen que no exista una sanción penal a los agentes que realizan actividades ilícita causando perjuicio económico, razón por la cual urge una modificación a la norma en la que se contemple al phishing como una figura delictiva actualizando de esta manera las normas penales.

Para responder al primer objetivo específico, doctrinariamente se ha obtenido lo siguiente: A decir de Terán (2016), quien refiere que en nuestro actual marco normativo hay vacíos que se evidencian, con la falta de tipificación del Phishing, toda vez que es nula la mención que se hace al phishing como figura delictiva en la ley de delitos informáticos, razón por la cual al existir esta carencia esta debe de ser revertida incluyendo esta nueva modalidad en el cuerpo legal antes descrito. En ese sentido a nivel doctrinario la ley de delitos informáticos en el Perú es ineficiente, dado que en el espíritu de la norma no se ha consagrado la inclusión del phishing como figura delictiva. La presente tesis se adhiere a lo suscrito por el mencionado autor, toda vez que en efecto nuestro marco normativo y doctrinario se evidencia las deficiencias que

imposibilitan que se sancionen penalmente a los responsables de estos actos ilícitos, que causan perjuicio económico a todas las personas que por desconocimiento de los avances tecnológicos.

A nivel de derecho comparado, nuestro país se encuentra rezagado a diferencia de todas naciones en materia de delitos informáticos quienes están más adelantados respecto a la figura delictiva del phishing por ende, el encuadramiento de la acción penal permite tener mayores resultados respecto a este tipo de delitos dado que si bien es cierto la conducta atípica de esta figura delictiva presupone la existencia de actos preparatorios para sancionar a los agentes que causen fraude con su actuar, se debe de considerar lo último para sancionarnos bajo la modalidad de phishing informático, el mismo que tiene un perfeccionamiento de esta conducta ilícita para obtener un provecho económico. Como antes lo había mencionado países de la región como lo es Ecuador, quien luego de una campaña de phishing informático se vio en la necesidad de incluir esta figura delictiva que busca recopilar todo tipo de información con el objetivo primordial de obtener con su actuar algún tipo de provecho, lesionando derechos de personas naturales como jurídicas con el objetivo de lucrar. Debemos de tomar en consideración que el phishing es más que un simple fraude es la fusión de varios delitos agrupados en una acción determinada a causar perjuicio económico, de datos personales e invasión de la privacidad, dada la esfera en la que se desarrolla se requiere una urgente modificación a las normas para sancionar de manera idónea este tipo de conductas ilícitas.

Ahora, considerando lo expresado por los entrevistados y tomando como punto de referencia el primer objetivo específico, relacionado con el aspecto normativo legal de la actualidad jurídica del phishing en el S.P.P., para la lucha contra la ciberdelincuencia, 2024. A decir de los participantes en mayoría sostienen que en efecto no existe norma legal que consagre postulado alguno que haga referencia al Phishing Informático en nuestro marco normativo. Del mismo al realizar una revisión de la ley de delitos informáticos se puede apreciar que el artículo más cercano a la imputación de esta nueva modalidad vendría a ser el fraude informático, sin embargo, este tiene poca relevancia penal, toda vez que no consagra el Phishing, como modalidad delictiva. Finalmente, una posición y opinión personal esto es relacionado con el primer objetivo específico, en nuestro país no está regulado o tipificado el

phishing como figura delictiva, razón por la cual se requiere que se sancione esta modalidad delictiva que tiene relevancia jurídica, debido a los índices de incrementos de estos delitos que surgen en la esfera tecnológica imposibilitando que se sancione correctamente esta nueva modalidad delictiva. Situación que debe de ser revertida con la posibilidad de sancionar a los agentes que realicen actos contrarios a la ley. Para ello se requiere una modificación a la actual norma legal para hacerle frente a este tipo de delitos informáticos ello debido a como lo he señalado en líneas precedentes se debe de incluir al phishing dentro de la ley de delitos informáticos, para luchar contra la ciberdelincuencia.

En referencia a los resultados referidos al *segundo O.E.* que versa sobre explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024, tomando en consideración la discusión con los antecedentes se ha obtenido lo siguiente: En primer lugar, a nivel normativo tenemos a Pardo (2018) concluye que existe deficiencia en el actual marco normativo y tal y como lo hemos dilucidado líneas más arriba en efecto afecte una norma deficiente que dificulta una sanción efectiva de aquellos delitos contra el patrimonio que se desarrollan en el espacio digital. Por todo lo señalado considero que se debe penalizar las nuevas modalidades de estos ilícitos penales. De esta manera se sancionarán estos delitos que tienen alta incidencia en nuestro país, en ese extremo, a la hora de perseguir el delito se deben de imputar correctamente estos nuevos tipos penales, de esta manera se podrá otorgar de protección en el ciberespacio que todas las operaciones financieras, se desarrollen con la seguridad necesaria, siguiendo esa línea a nivel doctrinario en referencia al segundo objetivo específico tenemos a decir de Gamio (2018) el patrimonio está orientado a obtener un fin económico ya que el patrimonio está constituido por bienes, derechos y acciones que se desarrolla de manera personal. En los delitos informáticos La teoría de los Bienes jurídicos afectados son el patrimonio toda vez que el sujeto activo busca lucrar con el desconocimiento de las personas que accede a las plataformas digitales previamente suplantadas por los cibercriminales, razón por la cual corresponde al estado proteger estos Bienes jurídicos los mismos que son supraindividuales.

Doctrinariamente tenemos a Hidalgo y Solano (2021) quienes señala que nuestro actual marco normativo no posee una norma con estas nuevas modalidades antes

descritas situación que pone en riesgo las transacciones financieras. Por ello urge profundizar en legislación doctrinaria que permita realizar un estudio más exhaustivo a esta nueva modalidad delictiva en nuestro país, ello debido principalmente por los altos índices de incidencia criminal de este tipo de delitos que como se ha mencionado en líneas precedentes existe un vacío legal para imputar este tipo de delitos. Situación que puede ser revertida con la dación de una norma que permita sancionar a los sujetos activos de la acción delictiva. Ahora, tomando en consideración lo mencionado por los entrevistados la mayoría de los entrevistados señalaron que, doctrinariamente la figura delictiva del Phishing en nuestro país es nula, razón por la cual para estudiar este tipo de modalidad o tipo se debe recurrir a legislación internacional, es decir que para abordar esta información se debe estudiar doctrinariamente consultando fuente internacional. En ese sentido es uniforme por parte de los entrevistados al señalar que existe un poco aproximación de delitos informáticos. Esto se puede confirmar con los altos índices de incidencia criminal que pone en riesgo a los ciudadanos.

Ahora, tomando posición y a manera de opinión personal y con referencia al segundo objetivo específico, se requiere tomar acción necesaria para poder modificar la ley de delitos informáticos para consagrar una norma que pueda imputar esta modalidad delictiva que causa perjuicio, se requiere que el actual marco legal sancione para poder perseguir este tipo de modalidad delictiva acciones para erradicar la impunidad de este tipo de delitos que dada las circunstancias en las que se desarrolla es casi imposible una sanción penal. Por ello se requiere un estudio más amplio a nivel doctrinario para tener una noción clara de cómo se desarrolla este tipo de delitos, los actos preparatorios de esta conducta ilícita.

En cuanto, a los resultados relacionados al *tercer O.E.* 3 derecho comparado y tomando en consideración la discusión con los antecedentes de la tesis, se ha obtenido lo siguiente: a nivel normativo a decir de Herrero (2021), en su investigación refiere que el Phishing es un delito nuevo que merece una tipificación idónea para erradicar la alta incidencia de estos delitos. En tal sentido es adecuado afirmar que estos delitos al desarrollarse en la esfera digital, la imputación para la obtención de las pruebas digitales es muy difícil de identificar a los agentes. Situación que debe ser revertida con la tipificación en nuestro ordenamiento jurídico. En ese sentido,

Terán (2016), concluyo en su investigación que se debe de añadir la figura jurídica de este delito dado que con una regulación idónea se protegerá a los usuarios y la incidencia de este delito disminuiría definitivamente al regular este nuevo delito, se podrá realizar un encuadramiento correcto a la hora de perseguir este delito. Adicional a ello, Zapata (2019) señala que existe ineficacia normativa respecto al Phishing ya que no hay un postulado general para la tipificación de este ilícito penal, de esta manera el autor nos da un panorama sobre estos delitos Señalando que las normas para hacerle frente al phishing son inadecuadas e insuficientes debido al carácter temporal de la norma, aunado a ello el poco conocimiento tecnológico contribuye a la realización de estos ilícitos penales. A decir de Flores (2017), las personas que son víctimas de los delitos de phishing creen que los mensajes y llamadas son de una entidad financiera, situación que pone en riesgo al consumidor quien de buena fe accede a un link que es aparentemente enviado por una entidad real sin embargo esta fue previamente suplantada para obtener información relevante para obtener algún provecho económico.

A nivel doctrinario tenemos lo expresado por Sowmya et al (2023), en su artículo nos señala la existencia de vulneración de las plataformas, para darle veracidad a la que ha sido previamente clonada para obtener algún provecho económico que causara perjuicio al sujeto pasivo del delito de phishing. Ahora, tomando en consideración lo mencionado por los entrevistados, puedo decir que los entrevistados han coincidido de manera uniforme, que en la actualidad doctrinariamente la figura delictiva de phishing es inexistente Se tiene que recurrir a doctrina internacional, la manera en la que se aborda el tema de delitos informáticos en la modalidad de phishing es nulo en nuestro país, o que genera que los operadores de derecho, no puedan ejercer de manera correcta la imputación de estos delitos situación que pone en riesgo el correcto funcionamiento del sistema penal peruano, a nivel doctrinario en nuestro país si bien es cierto los delitos informáticos tienen alta incidencia criminal, aun no existe una política criminal informática para sancionar a los agentes que realicen estos actos contrarios a nuestro marco normativo.

A nivel de derecho comparado se tiene a 4 países, como Chile, Brasil, México y Colombia, tienen legislación referente a los delitos informáticos y la figura delictiva de Phishing. Ahora, tomando posición y a manera de opinión personal y con referencia al

O.E 3, puedo decir que la actualidad jurídica del phishing a nivel doctrinario, se basa en la posibilidad de sancionar esta conducta delictiva, por ello se debe de señalar que en el ordenamiento jurídico peruano se debe de implementar de manera urgente la posibilidad de sancionar a los agentes que realicen conductas ilícitas, recogiendo información internacional que permita comparar legislaciones para integrar normas a nivel nacional tomando en consideración el convenio de Budapest que delimita que actuar de los miembros suscritos en el convenio antes señalado, ello con el objetivo de uniformar normas que puedan posibilitar la persecución penal.

V. CONCLUSIONES

En relación al O.E 1 que consistió en Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el S.P.P, para la lucha contra la ciberdelincuencia, 2024. Se concluye que la ley de delitos informáticos no consagra al Phishing como un tipo penal, solo hace referencia al fraude informático, pero debemos de tomar con consideración que con la implementación de una modificación a la ley se debería de incluir al phishing como un delito dentro de este marco normativo toda vez que al incluir esta figura jurídica se posibilitaría una correcta imputación y sanción penal dado que para la comisión de estos delitos se requiere actos preparatorios para conseguir el objetivo de los delincuentes informáticos lucrar. Situación que es confirmada por los entrevistados quienes en amplia mayoría refieren que existen vacíos legales respecto al actual marco normativo de la ley de delitos informáticos. Coincido con la postura de la existencia de un marco normativo ineficiente ello debido a los altos índices de criminalidad informática.

En relación al O.E. 2 que consistió en Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el S.P.P, para la lucha contra la ciberdelincuencia, 2024. Se concluye en nuestro país no existe fuente doctrinaria que haga mención al phishing. Razón por la cual se requiere una actualización de la norma para sancionar este tipo de delito que es novísimo en nuestra legislación. Esta información lo podemos confirmar con las entrevistas recabadas en la que los entrevistados refieren la carencia existente respecto a la doctrina que haga mención al phishing informático, solo existe doctrina que hace mención al fraude informático.

En relación al O.E. 3 que consistió en Explicar desde el derecho comparado es la actualidad jurídica del phishing en el S.P.P, para la lucha contra la ciberdelincuencia, 2024. según los artículos mencionados de distintos países este ilícito penal, tiene relevancia jurídica para la búsqueda de sanción penal. Si bien es cierto en la legislación antes descrita no se tipifica el phishing informático como tal, se debe de regular esta nueva figura que sancione esta conducta reprochable que busca generar perjuicio económico.

Tal y como se evidencia en las entrevistas realizadas a los especialistas estos refieren que en efecto se debe de recurrir al derecho comparado para tomar conocimiento de cómo operan los sujetos activos para cometer estos delitos, por ello al realizar un

análisis sobre la comparación de legislación se demuestra la carencia de falta de uniformar normas que permitan tener una arista clara respecto a estos delitos. En relación al objetivo general que consistió en analizar cuál es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

Se concluye que el escenario legal del phishing no se encuentra regulado en nuestra legislación, razón por la cual es desactualizada el actual marco normativo. Primero, por su falta de regulación normativa, ya que los artículos comprendidos en la ley de delitos informáticos no contemplan esta figura delictiva del phishing. Segundo, y esto en alusión a lo señalado anteriormente, la ley de delitos informáticos no consagra este tipo de modalidad que es más compleja toda vez que posee actos preparatorios para la comisión de ilícitos penales, causando perjuicio económico a las personas que son víctimas de estos ilícitos toda vez que no se puede imputar este tipo de delitos a los sujetos activos que comenten esta modalidad delictiva. Tercero, pese a la modificación de la ley de delitos informáticos, esta no ha consolidado un alto a los índices de fraude toda vez que no se imputa de manera idónea a nivel penal. Finalmente, como antes ya lo eh señalado nuestra actualidad jurídica requiere una solución inmediata con la dación de una norma que permita imputar a los sujetos activos de responsabilidad penal en la comisión de phishing informático, ello debido principalmente a los altos índices de criminalidad informática.

VI. RECOMENDACIONES

Se recomienda la elaboración de un proyecto de ley para sancionar a los delincuentes informáticos que realicen actos en contra de usuarios a las plataformas digitales con el objetivo de disminuir las tasas de criminalidad de estos delitos que están en auge constante, razón por la cual con la creación de un proyecto de ley se modificara el actual marco normativo haciendo la norma más idónea y eficiente para hacerle frente a la ciberdelincuencia. Se recomienda que los operadores de justicia deban de tener una capacitación constante respecto a cómo se llevan a cabo este tipo de delitos informáticos, de esta manera los operadores de justicia tendrán conocimiento pleno de como los agentes realizan las conductas ilícitas con el objetivo de causar un perjuicio económico a las víctimas.

Se recomienda la creación de una oficina descentralizada, de atención al usuario en la que se detecte información maliciosa respecto a presuntas operaciones financieras fraudulentas, se alerte sobre la suplantación de la identidad de las personas de la misma manera se bloquee las transacciones que dicha oficina considere fraudulentas hasta que el propietario de manera biométrica pueda autenticar que es quien realiza las acciones propias por ser titular de una cuenta bancaria, de redes sociales, de empresa. La persona que posee los datos puede solicitar al responsable el acceso gratuito al archivo, así como la actualización, la rectificación, la eliminación o la anulación de los datos. Se deben tomar las medidas de seguridad necesarias cuando se trata de datos sensibles cuyo archivo deberá estar autorizado por la ley o por la persona titular.

Se recomienda la creación de un observatorio de seguridad informática en la que se monitoree de manera adecuada las transacciones financieras que puedan ser sospechosas, dicho monitoreo consiste en alertar al ciudadano sobre posibles alertas de acceso ilegal a sus plataformas digitales financieras, así como también al acceso a sus redes sociales y mensajería telefónica.

REFERENCIAS

- Acosta, Benavides, García (2020). *Delitos Informáticos: Impunidad Organizacional Y Su Complejidad En El Mundo De Los Negocios*.
<https://www.redalyc.org/revista.oa?id=290>
- Álvarez. A (2020). *Clasificación de las investigaciones*. Universidad de Lima, Facultad de Ciencias Empresariales y Económicas, Carrera de Negocios Internacionales. <https://repositorio.ulima.edu.pe/handle/20.500.12724/10818>
- Astete, J. (Ed.). (2023). *Los delitos informáticos con mayor incidencia y los bancos más afectados*. diario gestión. <https://gestion.pe/peru/ciberataques-delitos-informaticos-con-mayor-incidencia-y-los-bancos-mas-afectados-mininter-gobierno-hackers-delincuentes-ciberneticos-noticia/>
- Cabrera, P. (2017). *Derecho Penal Parte Especial*. Lima: Moreno
- Espinoza (2017). *Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control*.
- Flores, C. (2017). *El phishing como comportamiento penalmente relevante*.
http://opac.pucv.cl/pucv_txt/txt-4000/UCC4478_01.pdf
- Fuentes Garrido, K. V. (2021). *Modificación de la Ley 30096 para incorporar los Delitos de Phishing, Pharming Y Carding como Delitos Penalizables con prisión, para reducir la ciberdelincuencia, Lima 2019* [Universidad Señor de Sipan].
- Gamio, A. (2018). *Límites a la creación voluntaria de patrimonio de afectación para la salvaguarda de bienes*. Revista de derecho de la universidad de Montevideo, 147.
- García Forero, L. F. G. (2020). *Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo*. [Tesis de grado. Universidad Piloto de Colombia].
<http://repository.unipiloto.edu.co/handle/20.500.12277/9545>
- García, V. (Ed.). (2019). *¿cómo está avanzando la ciberseguridad en el Perú? breve aproximación al marco normativo*. Actualidad Jurídica Uría Menéndez.

- Gupta, S., & Bansal, H. (2023). *Trust evaluation of health websites by eliminating phishing websites and using similarity techniques*. *Concurrency and Computation: Practice & Experience*, 35(21). <https://doi.org/10.1002/cpe.7695>
- Hanco, E. (2018), en su investigación titulada, *La Tipificación del Bien Jurídico Protegido en la Estructura del Tipo Penal Informático como causas de su deficiente regulación en la Ley 30096, Perú – 2017*. <http://repositorio.unsa.edu.pe/bitstream/handle/UNSA/6436/DEhazaey.pdf?sequence=1&isAllowed=y>
- Herrero, Torres, Vivas (2021). *Smartphone Addiction, Social Support, And Cybercrime Victimization: A Discrete Survival And Growth Mixture Model*. <https://www.redalyc.org/journal/1798/179870642005/>
- Hidalgo coronel, C. N., y Solano vidal, G. S. (2021). *El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano*. Propuesta de incorporación del artículo 7-a en la Ley de Delitos Informáticos 30096. [Tesis de 30 Grado, Universidad Nacional del Santa]. <http://repositorio.uns.edu.pe/handle/UNS/3849>
- Ley N° 30096 de 2013. *Ley de Delitos Informáticos*. 22 de octubre de 2013. Recuperado de <https://spij.minjus.gob.pe/spij-ext-web/detallenorma/H1088463>
- Ley N° 30171 de 2014. *Ley que modifica la Ley 30096, Ley de Delitos Informáticos*. 10 de marzo de 2014. <https://repositorio.umsa.bo/bitstream/handle/123456789/13890/T4774.pdf?sequence=1&isAllowed=y>
- López, J. (2019). *Métodos y técnicas de detección temprana de casos de phishing*, Cataluña, Universitat Oberta de Catalunya. <https://spij.minjus.gob.pe/spij-extweb/detallenorma/H1097704>
- Mayer, L. (2017). *El bien jurídico protegido en los delitos informáticos*. *Revista chilena de derecho*, 44(1), 261-285. Doi: <http://dx.doi.org/10.4067/S0718-34372017000100011>

- Mayer, L. (2018). *Elementos criminológicos para el análisis jurídico-penal de los delitos informáticos*. *Ius et Praxis*, 24(1), 159- 206. <https://dx.doi.org/10.4067/S0718-00122018000100159>
- Mayer, Oliver (2020). *El Delito De Fraude Informático: Concepto Y Delimitación*. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S071925842020000100151&lang=es
- Mengoá, M. (2021). *Punibilidad del comportamiento del phisher-mule en el delito de fraude informático en el Perú*. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/62379/Mengoá_VMM-SD.pdf?sequence=1
- Mori, F. (2019). *Los delitos informáticos y la protección penal de la intimidad en el distrito judicial de Lima, periodo 2008 al 2012*. http://repositorio.unfv.edu.pe/bitstream/handle/UNFV/3519/UNFV_MORI_QUIROZ_FRANCISCO_MAESTRIA_2019%20%283%29.pdf?sequence=1&isAllowed=y
- Opara, C., Chen, Y., & Wei, B. (2024). *Look before you leap: Detecting phishing web pages by exploiting raw URL and HTML characteristics*. *Expert Systems with Applications*, 236(121183), 121183. <https://doi.org/10.1016/j.eswa.2023.121183>
- Ortiz Campos, N. J. (Ed.). (2019). *Normativa Legal sobre Delitos Informáticos en Ecuador Legal Regulations on Cybercrimes in Ecuador* (Vols. 4, No. 1, 2019). Rev. Hallazgos21, <http://revistas.pucese.edu.ec/hallazgos21/>
- Palacios Rodríguez, Oscar Alejandro. (2021). *La teoría fundamentada: origen, supuestos y perspectivas*. *Intersticios sociales*, (22), 47-70. Epub 03 de noviembre de 2021. http://www.scielo.org.mx/scielo.php?script=sci_arttext&pid=S2007-49642021000200047&lng=es&tlng=es.
- Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima*, 2018. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y

- Paredes, J. (2017). *De los delitos cometidos con el uso de sistemas informáticos en el distrito judicial de Lima, en el período 2009-2010*.
https://cybertesis.unmsm.edu.pe/bitstream/handle/20.500.12672/10314/Paredes_pj.pdf?sequence=3&isAllowed=y
- Salvi, M. (2019) *El Phishing en la Argentina* [Tesis de Grado, Universidad Siglo 21].
<https://repositorio.uesiglo21.edu.ar/handle/ues21/16066>
- Shoab, M., & Umar, M. S. (2023). *An investigation in detection and mitigation of smishing using machine learning techniques. Social Network Analysis and Mining*, 13(1).
- Sowmya, Mary Anita, T. (2023) *International Journal of Intelligent Systems and Applications in Engineering*
- Tacilio Yauli, E. F. (2016). *Metodología de la Investigación Científica. Universidad Jaime Bausate y Meza*. Recuperado de
<http://repositorio.bausate.edu.pe/handle/bausate/36>
- Tellez Valdés, J. (2008). *Derecho Informático*. México: Editorial Graw Hill.
- Terán, T. (2016). *La necesidad de incorporar en el código penal el tipo penal de falsificación informática (Phishing)*.
- Tian, C. (annie), Jensen, M. L., & Durcikova, A. (2023). *Phishing susceptibility across industries: The differential impact of influence techniques. Computers & Security*, 135(103487), 103487. <https://doi.org/10.1016/j.cose.2023.103487>
- Tóala, G. M. T., y Briones, A. A. M. (2019). *Importancia de la enseñanza de la metodología de la investigación científica en las ciencias administrativas. Dominio de las Ciencias*, 5(2), 56-70
- Zapata, J. (2019). *El delito de estafa en la modalidad "Phishing" a través de internet y sus medios probatorios en Venezuela*. Universidad de Carabobo.

ANEXOS

ANEXOS 1: Matriz de Consistencia

Título: “La tipificación del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia.”

Problema	Objetivo	Supuesto	categorías	metodología
¿Cuál es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024?	Analizar cuál es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024	La actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, desde el aspecto normativo legal tiene vacíos legales e invita a interpretaciones descontextualizadas. Asimismo, desde el aspecto doctrinario, este viene siendo obsoleto y desactualizada y finalmente, desde el aspecto del derecho comparado se presenta de manera muy general.	Phishing	Enfoque: Cualitativo. Diseño de Investigación: Teoría fundamentada Tipo de estudio: Básica
P. Específico	O. Específico	S. Específico		
1.¿Desde el aspecto normativo legal cuál es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia?	1. Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.	1.La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano es deficiente por tiene vacíos legales e invita a interpretaciones descontextualizadas.	Sistema penal peruano	Técnica de investigación: la entrevista y el análisis documental Instrumento: documento normativo legal y doctrinario
2.¿Desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024?	2. Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.	2.La actualidad jurídica phishing en el sistema penal peruano, es deficiente ya que el mismo es obsoleto y desactualizada		
3.¿Desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024?	3. Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.	3.La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy apropiada porque es muy general.		

Elaboración propia 2024.

ANEXO 2

Instrumentos de investigación.

GUÍA DE ENTREVISTA

TÍTULO:

“La tipificación del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia.”

Entrevistado:.....

Cargo:.....

Institución:.....

OBJETIVO ESPECÍFICO 1

Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

Preguntas:

1. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?

.....
.....
.....
.....
.....

2. Desde su experiencia, Ud. cree que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas?.....

.....
.....
.....
.....

OBJETIVO ESPECÍFICO 2

Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

3. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto?.....
.....
.....
.....

4. Desde su experiencia, ud. cree La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano es desactualizada?.....
.....
.....
.....

OBJETIVO ESPECÍFICO 3

Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

5. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?
.....
.....
.....

Firma

GUÍA DE ANÁLISIS NORMATIVO

TÍTULO:

La tipificación del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia.

OBJETIVO ESPECÍFICO 1

Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

Nombre de la norma legal:				
Nombre del artículo	Artículo citado	Elementos a tomar en consideración	Interpretación	Calificación favorable o desfavorable

OBJETIVO ESPECÍFICO 2

Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

Nombre de la norma legal:				
Nombre del artículo	Artículo citado	Elementos a tomar en consideración	Interpretación	Calificación favorable o desfavorable

OBJETIVO ESPECÍFICO 3

Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

Nombre de la norma legal:				
Nombre del artículo	Artículo citado	Elementos a tomar en consideración	Interpretación	Calificación favorable o desfavorable

GUÍA DE ANÁLISIS DOCTRINARIO

TÍTULO:

La tipificación del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia.

OBJETIVO ESPECÍFICO 1

Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

AUTOR, TITULO, AÑO	CITA TEXTUAL	INTERPRETACION	CALIFICACION

OBJETIVO ESPECÍFICO 2

Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

AUTOR, TITULO, AÑO	CITA TEXTUAL	INTERPRETACION	CALIFICACION

OBJETIVO ESPECÍFICO 3

<p>Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024</p>
--

AUTOR, TITULO, AÑO	CITA TEXTUAL	INTERPRETACION	CALIFICACION

ANEXO 03

Ficha de validación

VALIDACIÓN DE INSTRUMENTOS

I. DATOS GENERALES

- 1.1. Apellidos y Nombres:
- 1.2. Cargo :
- 1.3. institución donde labora:
- 1.4. Nombre del instrumento: Guía de entrevista
- 1.5. Autor de Instrumento:

II. ASPECTOS DE VALIDACIÓN

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

II. OPINIÓN DE APLICABILIDAD

El Instrumento cumple con los Requisitos para su aplicación:

El Instrumento no cumple con Los requisitos para su aplicación:

III. PROMEDIO DE VALORACIÓN:

%

Validadores

Ficha de validación de contenido para un instrumento

INSTRUCCIÓN: A continuación, se le hace llegar el instrumento de recolección de datos (Guía de entrevista) que permitirá recoger la información en la presente investigación: “La tipificación del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia.”. Por lo que se le solicita que tenga a bien evaluar el instrumento, haciendo, de ser caso, las sugerencias para realizar las correcciones pertinentes. Los criterios de validación de contenido son:

Criterios	Detalle	Calificación
Suficiencia	El/la ítem/pregunta pertenece a la dimensión/subcategoría y basta para obtener la medición de esta	1: de acuerdo 0: en desacuerdo
Claridad	El/la ítem/pregunta se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas	1: de acuerdo 0: en desacuerdo
Coherencia	El/la ítem/pregunta tiene relación lógica con el indicador que está Midiendo	1: de acuerdo 0: en desacuerdo
Relevancia	El/la ítem/pregunta es esencial o importante, es decir, debe ser incluido	1: de acuerdo 0: en desacuerdo

Nota. Criterios adaptados de la propuesta de Escobar y Cuervo (2008).

Matriz de validación de la guía de entrevista de la primera categoría Phishing y la segunda categoría Sistema Penal Peruano.

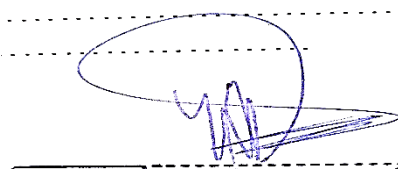
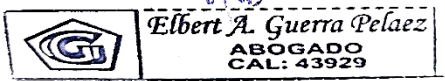
Zapata (2019) señala que existe ineficacia normativa respecto al Phishing ya que no hay un postulado general para la tipificación de este ilícito penal, de esta manera el autor nos da un panorama sobre estos delitos.

Validador 1

Categoría	Indicador	Preguntas	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Phishing Sistema penal peruano	Implementación	Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?	1	1	1	1	
	Conocimiento	Desde su experiencia, Ud. cree que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas	1	1	1	1	
	Aplicación	Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto	1	1	1	1	
	Conocimiento	Desde su experiencia, Ud. cree La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano es desactualizada	1	1	1	1	
	Aplicación	Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?	1	1	1	1	

FICHA DE VALIDACIÓN DE JUICIO DE EXPERTO

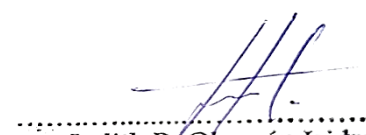
Nombre del instrumento	Guía de entrevista
Objetivo del instrumento	Recoger información para responder el objetivo específico 1
Nombres y apellidos del experto	Erberth A. Guerra Pelaez
Documento de identidad	
Años de experiencia en el área	20
Máximo Grado Académico	Doctor
Nacionalidad	Peruano

Institución	GUELSAC.
Cargo	Abogado y gerente
Número telefónico	
Firma	 
Fecha	10/10/23

Validador 2

Categoría	Indicador	Preguntas	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Phishing	Implementación	Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?	1	1	1	1	
	Conocimiento	Desde su experiencia, Ud. cree que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas	1	1	1	1	
	Aplicación	Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto	1	1	1	1	
	Conocimiento	Desde su experiencia, Ud. cree La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano es desactualizada	1	1	1	1	
	Sistema penal peruano	Aplicación	Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?	1	1	1	1

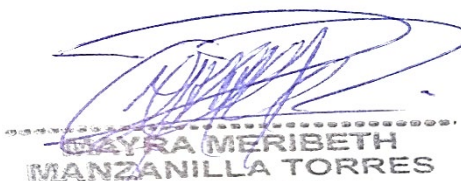
--	--	--	--	--	--	--	--

Nombre del instrumento	Guía de entrevista
Objetivo del instrumento	Recoger información para responder el objetivo específico 1
Nombres y apellidos de experto	Judith B. Obregón Isidro
Documento de identidad	
Años de experiencia en el área	10
Máximo Grado Académico	Colegiada
Nacionalidad	Peruano
Institución	gupelsac
Cargo	Magister
Número telefónico	
Firma	 Judith B. Obregón Isidro ABOGADA C.A.L. N° 71270
Fecha	10/05/24

Validador 3

Categoría	Indicador	Preguntas	Suficiencia	Claridad	Coherencia	Relevancia	Observación
Phishing	Implementación	Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?	1	1	1	1	
	Conocimiento	Desde su experiencia, Ud. cree que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas	1	1	1	1	

Sistema penal peruano	Aplicación	Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto	1	1	1	1	
	Conocimiento	Desde su experiencia, Ud. cree La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano es desactualizada	1	1	1	1	
	Aplicación	Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?	1	1	1	1	

Nombre del instrumento	Guía de entrevista
Objetivo del instrumento	Recoger información para responder el objetivo específico 1
Nombres y apellidos de experto	Mayra Meribeth Manzanilla Torres
Documento de identidad	46318810
Años de experiencia en el área	04
Máximo Grado Académico	Licenciada
Nacionalidad	Peruana
Institución	
Cargo	
Número telefónico	
Firma	 <p>MAYRA MERIBETH MANZANILLA TORRES ABOGADA REG. CAL. 86333</p>
Fecha	10/04/24

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

- 1.1. Apellidos y Nombres: Mg. Ríos Inga, Gabriela Mercedes
- 1.2. Cargo e institución donde labora: Especialista de Audiencias en la Corte Superior de Justicia del Callao Poder Judicial del Perú
- 1.3. Nombre del instrumento motivo de evaluación: Guía de entrevista
- 1.4. Autor(A) de Instrumento: Peralta Huamán, Alex Jaime

II. ASPECTOS DE VALIDACIÓN

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

III. OPINIÓN DE APLICABILIDAD

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

Si

.....

IV. PROMEDIO DE VALORACIÓN:

95 %



PODER JUDICIAL DEL PERU
 GABRIELA MERCEDES RÍOS INGA
 DNI: 47427120
 ESPECIALISTA DE AUDIENCIAS
 JUZGADO DE INVESTIGACIÓN PREPARATORIA DEL SCJP
 CORTE SUPERIOR DE JUSTICIA DEL CALLAO

Lima, 07 de setiembre del 2023

FIRMA DEL EXPERTO INFORMANTE
 DNI No 47427120 Telf.: 960670306

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

- 1.1. Apellidos y Nombres: *HERNÁNDEZ EDUARDO ANDRÉS*
 1.2. Cargo e institución donde labora: *DOCENTE TIEMPO PARCIAL UCV-ATE*
 1.3. Nombre del instrumento motivo de evaluación: *Guía de entrevista*
 1.4. Autor(A) de Instrumento: *Peralta Huaman Alex Jaime*

II. ASPECTOS DE VALIDACIÓN

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

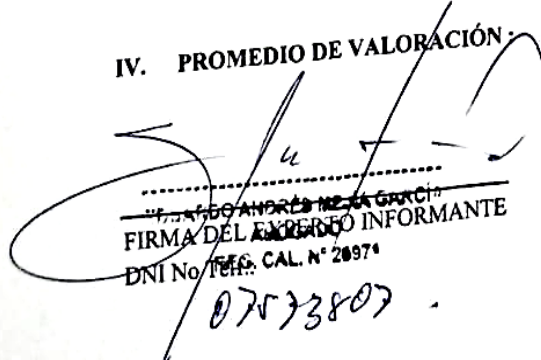
III. OPINIÓN DE APLICABILIDAD

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

90 %

IV. PROMEDIO DE VALORACIÓN:

u


 FIRMADO POR: *EDUARDO ANDRÉS HERNÁNDEZ*
 FIRMA DEL EXPERTO INFORMANTE
 DNI No. *07533807* TEF. CAL. N° 20974

Lima, 23 de noviembre del 2023

ANEXO 4

Base de datos

Matriz de comparación de datos e interpretación de resultados

3.1. Descripción de los resultados

Descripción de resultados: técnica de la entrevista

A continuación, se realizará la descripción de los resultados obtenidos en la presente tesis, utilizando la técnica de la entrevista, por ello el presente apartado inicia con los resultados obtenidos y vinculados al **objetivo específico 1**, el mismo que busca Explicar desde el aspecto normativo legal cuál es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

Siendo los siguientes resultados.

Tabla 1

Respuesta de los entrevistados a la 1ra pregunta

1. Pregunta 01: Ud. considera que ¿La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?	
Categoría: Phishing	
Subcategoría: Normativa Legal	
entrevistados	Respuesta de los entrevistados
Entrevistado 1 Sandra Vilchez	<u>Existen vacíos legales, (no hay una regulación sobre el phishing)</u> , ya que a la fecha no hay una regulación de las normas penales respecto al phishing como una nueva modalidad delictiva.
Entrevistado 2 Elbert Guerra	Actualmente no, <u>nuestro marco normativo no menciona la figura phishing</u> y eso hace que no haya una correcta imputación ante esta modalidad.
Entrevistado 3 Guillermo LLeren	En efecto, <u>nuestro cuerpo legal no contempla la figura legal del Phishing</u> , por ende, a la hora de perseguir este delito no existe una correcta imputación de esta nueva modalidad delictiva.
Entrevistado 4 Huber Gómez	En nuestro marco normativo no está tipificado la figura legal del phishing, por lo tanto, en el momento de perseguir este delito no va existir una adecuada norma para poder ser juzgada.
Entrevistado 5 Gustavo Castillo	<u>Nuestro marco normativo no cuenta con la regulación adecuada</u> , es por eso que el momento en que va a ser juzgado este delito no existe una correcta imputación de modalidades delictivas.
Entrevistado 6 Mayra Manzanilla	Es saber que nuestro cuerpo legal no contempla la figura que es phishing, es así que en el momento de castigar esta modalidad no hay una correcta imputación de esta modalidad delictiva.
Entrevistado 7	En la actualidad no, ya que con la última modificatoria de la ley de delitos informáticos en su art. 8 ya está regulado

Judith Obregón	
----------------	--

Análisis de la primera pregunta

A continuación, analizare las respuestas de los entrevistados en cuanto a la primera pregunta de la presente tesis a partir de ello se obtuvo como resultados que los entrevistados Vilchez, Gómez y Guerra, señalaron que existen vacíos legales respecto a la figura delictiva de phishing informático, por ende, señalan que no hay una correcta imputación de esta figura delictiva; mientras que LLeren, Manzanilla , Castillo, nos refieren que el actual marco normativo legal no contempla una regulación idónea respecto a este tipo de delitos, toda vez que la norma legal vigente solo contempla al fraude informático. Opinión contraria la conseguimos por parte de Oliva, quien refiere que la ley de delitos informáticos con la nueva modificación contempla esta figura delictiva de Phishing. Como podemos observar y a manera de conclusión que la mayoría de entrevistados seis de siete de ellos señalaron que la actualidad jurídica del Phishing presenta vacíos legales, pese a la modificación de la ley de delitos informáticos.

Tabla 2

Extracto y resumen de respuestas a la 1ra pregunta

Entrevistados	Extracto	Resumen	Supuesto
Entrevistado 1 Sandra Vilchez	Existen vacíos legales, (no hay una regulación sobre el phishing) ...	Los entrevistados señalan en mayoría que no existe una norma legal que permita encuadrar el Phishing en nuestro ordenamiento jurídico.	Desfavorable
Entrevistado 2 Elbert Guerra	... nuestro marco normativo no menciona la figura phishing...		
Entrevistado 3 Guillermo LLeren	...nuestro cuerpo legal no contempla la figura legal del Phishing...		
Entrevistado 4 Huber Gómez	En nuestro marco normativo no está tipificado la figura legal del phishing...		

Entrevistado 5 Gustavo Castillo	Nuestro marco normativo no cuenta con la regulación adecuada...		
Entrevistado 6 Mayra Manzanilla	... nuestro cuerpo legal no contempla la figura que es phishing...		
Entrevistado 7 Judith Obregón	...En la actualidad no...en su art. 8 ya está regulado...	Un entrevistado señala lo contrario.	Favorable

Ahora bien, en esa dirección por responder objetivo específico 1 se plantea la segunda pregunta de investigación: 2. Desde su experiencia, Ud. ¿Cree que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas? Se han obtenido los siguientes resultados producto de las entrevistas realizadas a los especialistas en Derecho Penal.

Tabla 3

Respuesta de los especialistas en derecho penal a la 2da pregunta

Desde su experiencia, Ud. cree que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas.	
Categoría: Phishing	
Subcategoría: Normativa legal	
entrevistados	Respuesta de los entrevistados
Entrevistado 1 Sandra Vilchez	Exacto el encuadramiento y tratamiento que se le da en la actualidad es de fraude informático sin embargo el phishing va más allá que ese solo aspecto jurídico
Entrevistado 2 Elbert Guerra	Sí, debido que no hay una interpretación clara de la norma, por eso se dice que hay vacíos legales para su correcta ejecución.
Entrevistado 3 Guillermo LLeren	Si debido principalmente a que no hay una interpretación normativa, por ende, hay vacíos legales para el correcto funcionamiento legal, por ello no hay una contextualización idónea de estos delitos.
Entrevistado 4 Huber Gómez	Si, ya que no hay una interpretación normativa correcta, es por ello que existen los vacíos legales para su correcto uso legal, y es así que no hay un correcto entendimiento de esta nueva modalidad.
Entrevistado 5 Gustavo Castillo	Si, debido a que no está una correcta interpretación adecuada de esta modalidad, es así que hay vacíos legales por lo cual no va a ver un correcto conocimiento sobre ella.

Entrevistado 6 Mayra Manzanilla	Si, por la razón que no hay una interpretación correcta la cual va hacer que hay vacíos legales para su correcta interpretación y por lo cual no hay una contextualización idónea.
Entrevistado 7 Judith Obregón	Considero que no ya que los verbos rectores son además que el tipo penal presenta situaciones como lo es la manera deliberada e ilegítima.

Análisis de la segunda pregunta

A continuación, analizaremos las respuestas de los entrevistados en cuanto a la segunda pregunta de la presente tesis. En ese sentido Vilchez y Guerra señalaron que no existe un tratamiento jurídico idóneo por ello a la hora de imputar este tipo de delitos solo se realiza de acuerdo a lo establecido en la ley de delitos informáticos como fraude. Por otro lado, el entrevistada LLeren va más allá y señala que la ley de delitos informáticos pese a una reciente modificatoria muestra una descontextualización y ello se debe a la inexistencia de una interpretación normativa. Gómez, Castillo y Manzanilla señalaron que existe una mala interpretación de la norma causando vacíos legales. Una opinión contraria la vemos en Obregón quien señala que con la nueva modificación de la ley de delitos informáticos se ha superado la carencia de existencia de una norma que describa este tipo penal.

Como podemos observar y a manera de conclusión que la gran mayoría de entrevistados para ser exactos seis de siete de ellos señalaron que existen vacíos legales respecto al actual marco normativo.

Tabla 4

Extracto y resumen de respuestas a la 2da pregunta

entrevistados	Extracto	Resumen	Supuesto
Entrevistado 1 Sandra Vilchez	No existe un tratamiento jurídico idóneo.	Los entrevistados señalan en mayoría que los artículos que van del 472 al 487 del código civil no refiere que la	Desfavorable
Entrevistado 2 Elbert Guerra	No existe una interpretación clara de la norma.		

Entrevistado 3 Guillermo Lleren	Existen vacíos legales por ende no existe una imputación objetiva idónea.	pensión de alimentos deba obtenerse desde la presentación de la demanda sino desde la admisión a trámite. Por lo tanto, no terminarían favoreciendo al alimentista.	
Entrevistado 4 Huber Gómez	No existe un correcto entendimiento de la nueva modalidad delictiva del Phishing.		
Entrevistado 5 Gustavo Castillo	No hay regulación sobre el Phishing.		
Entrevistado 6 Mayra Manzanilla	La norma actual esta descontextualizada		
Entrevistado 7 Judith Obregón	Considera idóneo el actual marco normativo.	Un entrevistado se encuentra a favor	Favorable

Tabla 5
resultados del objetivo específico 1

Preguntas	Favorable	Desfavorable
Ud. ¿Considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?	Un entrevistado refiere que el actual marco normativo, al tener una modificatoria contempla la figura delictiva del Phishing informático por ende no existe vacío legal ni invita a una descontextualización.	Los entrevistados en mayorías sostienen que existen vacíos legales en la ley de delitos informáticos.
Desde su experiencia, Ud. ¿Cree que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas?		Seis de siete entrevistados refiere que el sistema penal peruano invita a interpretaciones descontextualizadas respecto al phishing.

Respecto a los resultados vinculados al objetivo específico 2 que consiste en Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano para la lucha contra la ciberdelincuencia, 2024. En consecuencia, se han obtenido los siguientes resultados a partir de la tercera pregunta: Ud. ¿Considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto?

Tabla 6
Respuesta de las autoridades encargadas a la 3ra pregunta

Pregunta 3: Ud. ¿Considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto?

Categoría: Sistema Penal Peruano	
Subcategorías: Doctrina	
entrevistados	Respuesta de los entrevistados
Entrevistado 1 Sandra Vilchez	No hay doctrina que defina el Phishing como tal lo que existe es una visión general sobre estos delitos informáticos.
Entrevistado 2 Elbert Guerra	Doctrinariamente la información sobre el phishing es escasa en nuestro país y es por ello que se recurre a información o fuentes doctrinarias internacionales.
Entrevistado 3 Guillermo LLeren	Doctrinariamente existe poca información respecto al Phishing informático en nuestro país razón por la cual para recurrir a información doctrinaria se tiene que acudir a información extranjera
Entrevistado 4 Huber Gómez	De acuerdo a la normativa existe una mínima información clara sobre el phishing en nuestro país, es por ello se recurre siempre a fuentes extranjeras.
Entrevistado 5 Gustavo Castillo	En nuestro marco legal existe poca información respecto a esta modalidad que es phishing, es así que siempre se va acudir a doctrinas extranjeras, donde que estas tipificadas y reguladas dentro de su marco legal.
Entrevistado 6 Mayra Manzanilla	En nuestra doctrina existe una delimitada información y es por esta razón recurrir a información doctrinaria extranjera para su fácil entendimiento.
Entrevistado 7 Judith Obregón	Considero que, si ya que la doctrina nacional existe poca información de los delitos informáticos y más, aunque a la fecha se tiene una modificatoria que regula este aspecto.

Análisis de la tercera pregunta

En este caso todos los entrevistados han señalado que se obtuvo como resultados que la mayoría de los entrevistados (Vilchez, Guerra , LLeren, Manzanilla, Gómez Obregon) señalaron que Doctrinariamente la figura delictiva del Phishing en nuestro país es nula, razón por la cual para estudiar este tipo de modalidad o tipo se debe de recurrir a legislación internacional, es decir que para abordar esta información se debe de estudiar doctrinariamente consultando fuente internacional. En ese sentido es uniforme por parte de los entrevistados al señalar que existe un poco aproximación de delitos informáticos.

Tabla 7

Extracto y resumen de respuestas a la 3ra pregunta

entrevistados	Extracto	Resumen	Supuesto
---------------	----------	---------	----------

Entrevistado 1 Sandra Vilchez	No existe doctrina nacional que refiera la existencia del Phishing en nuestra legislación	Los entrevistados señalan que doctrinariamente la información es insuficiente razón por la cual no se puede profundizar sobre este tema	Desfavorable
Entrevistado 2 Elbert Guerra	Doctrinariamente la información sobre el phishing es inexistente.		
Entrevistado 3 Guillermo LLen Perez	Doctrinariamente la información es inexistente para profundizar sobre el estudio del Phishing en nuestro país.		
Entrevistado 4 Huber Gómez	La información es mínima en nuestro país.		
Entrevistado 5 Gustavo Castillo	Doctrinariamente el estudio sobre el Phishing es insuficiente.		
Entrevistado 6 Mayra Manzanilla	La doctrina es delimitada en nuestro país.		
Entrevistado 7 Judith Obregón	Existe poca información doctrinaria respecto al Phishing.		

Ahora bien, en ese sentido para responder objetivo específico 2 se plantea la cuarta pregunta de investigación: en referencia a la actualidad jurídica, Desde su experiencia, Ud. ¿cree La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano es desactualizada.

Se han obtenido los siguientes resultados producto de las entrevistas a los abogados especialistas.

Tabla 8

Respuesta de los abogados especialistas a la 4ta pregunta

Pregunta 4: Desde su experiencia, Ud. ¿Cree La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano es desactualizada?	
Categoría: Sistema Penal peruano	
Subcategoría: Doctrina	
entrevistados	Respuesta de los entrevistados

Entrevistado 1 Sandra Vilchez	Completamente es un delito o modalidad que esta en constante avance dada la clandestinidad en la que se da, razón por la cual no se imputan correctamente este tipo de delitos.
Entrevistado 2 Elbert Guerra	De acuerdo a nuestra actualidad jurídica no hay una norma legal vigente que nos permite tener una información de carácter eficaz, por eso se dice que el phishing no está regulado en nuestro sistema legal peruano.
Entrevistado 3 Guillermo LLeren Perez	No existe una norma legal vigente que nos permitan tener una información de carácter legal vigente, la norma sobre el phishing no esta regulada en nuestro sistema penal peruano
Entrevistado 4 Huber Gómez	No existe dentro de nuestro marco normativa una información legal vigente que nos va a permitir una información sobre el phishing, por una sencilla razón que no está regulado en nuestro marco normativo.
Entrevistado 5 Gustavo Castillo	No existe una norma legal contemplada que nos facilite información idónea, es así que no está normada dentro de nuestro sistema legal peruano.
Entrevistado 6 Mayra Manzanilla	En nuestra Doctrina no hay norma legal que nos brinde una información legal, la norma sobre el phishing no está regulada en nuestro sistema legal peruano.
Entrevistado 7 Judith Obregon	Considero que sí, ya que la realidad en la que vive el Perú, va en cambiando y las normas en atención a las relaciones sociales, es que se modifican y o incorporan nuevos tipos penales y en ese sentido la doctrina se ve desactualizada ya que no existe mayor tratamiento del delito.

Análisis de la cuarta pregunta

A continuación, analizaremos las respuestas de los entrevistados en cuanto a la cuarta pregunta del trabajo de investigación. En ese sentido Vilchez, Guerra, Lleren, Manzanilla, Gómez, Castillo y Obregón refirieron de manera uniforme que Doctrinariamente no hay mucha información respecto al Phishing situación que pone en riesgo futuras imputaciones a sujetos activos que realicen actividades ilícitas,

Tabla 9

Extracto y resumen de respuestas a la 4ta pregunta

entrevistado s	extracto	Resumen	Supuesto
Entrevistado 1 Sandra Vilchez	La norma esta desactualizada completamente es un delito o modalidad que está en constante avance dada la clandestinidad	Los entrevistados señalan que esta	Vulnerante

Entrevistado 2 Elbert Guerra	El Phishing no está regulado en nuestro sistema legal peruano.	Doctrinariamente es obsoleta ello debido principalmente por carecer de información.	
Entrevistado 3 Guillermo Lleren	El phishing no está regulado doctrinariamente en nuestro sistema penal peruano		
Entrevistado 4 Huber Gómez	No hay doctrina está regulado en nuestro marco normativo.		
Entrevistado 5 Gustavo Castillo	No existe una norma legal contemplada que nos facilite información idónea		
Entrevistado 6 Mayra Manzanilla	En nuestra Doctrina no hay norma legal que nos brinde una información legal		
Entrevistado 7 Judith Obregón	La doctrina se ve desactualizada ya que no existe mayor tratamiento del delito.		

Tabla 10

resultados del objetivo específico 2.

Preguntas	No vulnerable	Vulnerable
<p>1. Ud. ¿considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto?</p> <p>2. Desde su experiencia, Ud. ¿cree La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano es desactualizada.</p>		De manera uniforme, los encuestados han llegado a la conclusión que en la actualidad doctrinariamente la figura delictiva de phishing es inexistente

Con respecto a los resultados vinculados al **objetivo específico 3** que consistió en Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024. En consecuencia, se han obtenido los siguientes resultados a partir de la quinta pregunta: Ud. considera que La

actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?

Tabla 11

Respuesta de las autoridades encargadas a la 5ta pregunta

2. Pregunta 5: Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?	
Categoría: Sistema Penal peruano	
Subcategoría: Comparado	
entrevistados	Respuesta de los entrevistados
Entrevistado 1 Sandra Vilchez	El abordaje que se le da no es el idóneo por ende merece una regulación necesaria en la que se defina si es un tipo o una modalidad y cuáles son los elementos para considerarlos como delitos informáticos. Si esta abordado de manera general.
Entrevistado 2 Elbert Guerra	La regulación comparada nos ayuda tener una amplia información de como los países que ya están reguladas en su marco normativo, gracias a ellos vamos tener una visión de cómo se imputan estos ilícitos paso a paso y un adecuado juzgamiento.
Entrevistado 3 Guillermo LLeren	La regulación comparada nos permite tener una visión más amplia de cómo se imputan estos ilícitos, dado que nos señala los actos preparatorios para la consumación de estos delitos.
Entrevistado 4 Huber Gómez	La regulación comparada nos va a permitir una amplia información de estos delitos y los marcos normativos extranjeras que ya están regulados nos va visualizar de cómo deben ser juzgados estos delitos.
Entrevistado 5 Gustavo Castillo	Tomando, como base el derecho comparado podemos ver las falencias en nuestra norma penal, en diferentes países el delito de phishing ya se encuentra tipificado en su norma penal lo que facilita su juzgamiento y prevención del mismo. En el caso concreto, México tiene penal de cárcel para aquellos que accedan a la información contenida en sistemas o equipos informáticos del sistema financiero los que tiene protección a través de mecanismos que son vulnerados por los delincuentes.
Entrevistado 6 Mayra Manzanilla	La regulación comparada nos dará detalles y nos va permitir una visión amplia de cómo van a ser imputados estos ilícitos penales, en diferentes países el delito de phishing ya se encuentra tipificado en su norma penal lo que facilita su juzgamiento y prevención del mismo.
Entrevistado 7 Judith Obregón	Considero que sí, ya que en otros países a lo mejor las modificatorias de las normas penales van acorde a la jurisprudencia y la doctrina sobre los tipos de delitos informáticos y en el caso en concreto sobre el Phishing.

Análisis de la quinta pregunta

A continuación, analizaremos las respuestas de los entrevistados en cuanto a la quinta pregunta del trabajo de investigación. se obtuvo como resultados que todos los entrevistados refieren que los procesos de alimentos en el Perú si son lesivos y van en contra del menor toda vez que dicho proceso es lento e ineficiente. Llanos agrega a manera de recomendación que no se puede desamparar estos tipos de procesos al

tratarse de la subsistencia de las personas. Rojas, reflexiona respecto a estas demoras judiciales y concluye que estas mismas no se deben tanto a la ley en sí, sino a los operadores de justicia que en su momento no se generan trabajo orquestados de tal manera que permita una mayor velocidad de las calificaciones de las demandas.

Tabla 12

Extracto y resumen de respuestas a la 5ta pregunta

entrevistado s	extracto	Resumen	Supuesto
Entrevistado 1 Sandra Vilchez	El abordaje que se le da no es el idóneo.	Los entrevistados señalaron que el delito de Phishing esta regulado de manera general, sin embargo, se debe de recurrir a estos medios para recabar información sobre delitos de Phishing	Vulnerante
Entrevistado 2 Elbert Guerra	La regulación comparada nos ayuda tener una amplia información de cómo los países que ya están reguladas en su marco normativo.		
Entrevistado 3 Guillermo LLeren	La regulación comparada nos permite tener una visión más amplia de cómo se imputan estos ilícitos.		
Entrevistado 4 Huber Gómez	La regulación comparada nos va a permitir una amplia información de estos delitos.		
Entrevistado 5 Gustavo Castillo	El delito de phishing ya se encuentra tipificado en su norma penal lo que facilita su juzgamiento y prevención del mismo		
Entrevistado 6 Mayra Manzanilla	La regulación comparada nos dará detalles y nos va permitir una visión amplia de cómo van a ser imputados estos ilícitos penales		
Entrevistado 7 Brandon Oliva Ramos	las modificatorias de las normas penales van acorde a la jurisprudencia y la doctrina.		

Tabla 13

Resultados del objetivo específico 3

Preguntas	No vulnerante	Vulnerante
-----------	------------------	------------

Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?

No existe información nacional

Los entrevistados señalaron que a nivel comparado existe legislación que sirve de base para que el estado pueda sancionar las actividades ilícitas ejecutadas por el agente.

Con respecto al instrumento del análisis documental: normativa legal, se considera y con respecto al objetivo específico 1 Existen vacíos legales respecto al actual marco normativo legal pese a una reciente modificación.

Con respecto al instrumento del análisis documental: normativa legal, se considera y con respecto al objetivo específico 2. De manera uniforme, los encuestados han llegado a la conclusión que en la actualidad doctrinariamente la figura delictiva de phishing es inexistente.

En referencia al instrumento del análisis documental: normativa legal, se considera y con respecto al objetivo específico 3. Los entrevistados señalaron que a nivel comparado existe legislación que sirve de base para que el estado pueda sancionar las actividades ilícitas ejecutadas por el agente.

Técnica de análisis documental

A continuación, se desarrollará instrumento de guía de revisión normativa legal, para responder el objetivo específico 1, el mismo que pretende Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

REVISIÓN DE LA NORMATIVA LEGAL

TÍTULO:

La tipificación del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia.

OBJETIVO ESPECÍFICO 1

Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

Tipo de norma legal y año de emisión	Cita	Interpretación	Calificación
--------------------------------------	------	----------------	--------------

<p>ley de delitos informáticos ley n.º 30096</p>	<p>El que accede sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa.</p>	<p>Como se puede apreciar en el artículo 2 de la ley de delitos informáticos, hace referencia al acceso de manera ilícita del sistema financiero.</p>	<p>Aplicable</p>
<p>ley de delitos informáticos ley n.º 30096</p>	<p><i>delitos contra el patrimonio.</i> art. 8 fraude informático</p> <p>El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.</p>	<p>El fraude es la acción por la cual un tercero suplanta la información de una página web con el objetivo de aprovecharse económicamente de una persona haciéndole creer que se encuentra en una aplicación real cuando es falsa, cuyo objetivo es recabar su información para lucrar.</p>	<p>Inaplicable</p>
<p>ley de delitos informáticos ley n.º 30171 10 de marzo de 2014</p>	<p><i>delitos contra el patrimonio</i></p> <p>Artículo 8. Fraude informático El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, suplantación de interfaces o páginas web o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de cuatro ni mayor de ocho años y con sesenta a ciento veinte días-multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.</p>	<p>Hace referencia a que una persona de manera ilegítima pueda acceder a medios tecnológicos para obtener provecho económico de personas que desconocen de la tecnológico.</p>	<p>Aplicable</p>

CONCLUSIÓN: En esta línea, los delitos informáticos actualmente se encuentran regulados mediante la Ley N°30096, no obstante, persisten diversos vacíos legales,

toda vez que no todos los delitos se han abordado en dicha normativa, teniendo en cuenta que existen nuevas formas de delinquir a través del sistema informático.

A continuación, se desarrollará instrumento de guía de revisión doctrinaria, para responder el objetivo específico 2, el mismo que pretende Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

GUÍA DE ANÁLISIS DE REVISIÓN DE FUENTE DOCTRINARIA

TÍTULO

La tipificación del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia.

OBJETIVO ESPECÍFICO 2

Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

Autor, Año, página	Cita textual	Interpretación	Calificación
Valle Matute Juan(2017, p.125)	Señala que, debido al aumento del fraude, Ecuador se ha ido adaptando a las nuevas conductas delictivas que se realizan en el espacio digital Esta situación pone en manifiesto los avances del delito de phishing como fraude.	El autor señala que existe una novísima modalidad delictiva que surge en la esfera de la era tecnológica, razón por la cual la actualización de normas legales permitirá hacerle frente a esa nueva modalidad delictiva.	Desactualizada
Herrero, (2021, p.75)	Herrero (2021), en su investigación refiere que el fraude es un delito nuevo que merece una tipificación idónea para erradicar la alta incidencia de estos delitos.	En tal sentido es adecuado afirmar que estos delitos al desarrollarse en la esfera digital, la imputación para la obtención de las pruebas digitales es muy difícil de identificar a los sujetos activos. Situación que debe de ser revertida con la tipificación en nuestro ordenamiento jurídico	Desactualizada
Zapata, (2019, p.30)	señala que existe ineficacia normativa respecto al fraude ya que no hay un postulado general para la tipificación de este ilícito penal.	De esta manera el autor nos da un panorama sobre estos delitos Señalando que las normas para hacerle frente al fraude son inadecuadas e insuficientes debido al carácter temporal de la norma, aunado a ello el poco conocimiento tecnológico contribuye a la realización de estos ilícitos penales	Desactualizada

Flores. (2017, p.43)	Las personas que son víctimas de los delitos de fraude creen que los mensajes y llamadas son de una entidad financiera, situación que pone en riesgo al consumidor quien de buena fe accede a un link que es aparentemente enviado por una entidad real sin embargo esta fue previamente suplantada para obtener información relevante para obtener algún provecho económico. (p.43)	El fraude, hace referencia a los medios por los cuales se vale el sujeto activo para la comisión de estos delitos, en tal sentido el autor nos señala una serie de actos preparatorios para cometer este delito informático.	Desactualizada
Vera Martino, Tapia (2023, p.14)	“Con el avance de la tecnología médica, han surgido dilemas éticos y legales sobre la posibilidad de poner fin a la vida de una persona por razones médicas o personales. Algunos argumentan que la eutanasia es una manera de asegurar que todos tengan derecho a una muerte tranquila y digna, especialmente cuando están sufriendo de enfermedades terminales o dolores extremos.”	El autor señala que en la actualidad se sigue debatiendo si es bueno aplica o no la eutanasia. Por lo tanto, sigue en tela de juicio la afectación o no de los derechos fundamentales de la persona.	Desactualizada
Paredes (2017, p.248)	El autor señala que al existir vacíos legales respecto al fraude los delitos se siguen cometiendo generando perjuicio a la ciudadanía. Situación que debe de ser revertida con una correcta imputación de este delito.	A decir del autor estos delitos tienen incidencia dado que no existe legislación uniforme para encuadrar estos delitos.	Actualizada
Cabrera (2017, p.43)	Cabrera (2017) señala que la Teoría constitucionalista, respecto al delito informático, se encuentra asentada básicamente en la protección constitucional de bienes jurídicos que se encuentran protegidos por la constitución política del estado, es decir que la lesión que se cause debe estar orientada a los derechos establecidos en nuestra carta magna.	Como es de conocimiento general, las nuevas tecnologías han traído desarrollo, pero a su vez tienen situaciones que han generado perjuicio, ya que la criminalidad informática está en constante desarrollo debido al poco conocimiento de esta importante herramienta	Desactualizada
Téllez Valdés (2008, p.40)	sostiene que la Teoría clásica, está orientada a identificar las acciones que realice el sujeto activo en la comisión del delito informático de fraude el mismo que debe de ser es típica antijurídica y culpable, si no cumplan con estos elementos no	La teoría clásica nos da una arista elemental respecto a la manera en la que se desarrolla este ilícito penal. Es decir que el actuar del sujeto activo debe de ser antijurídica y culpable.	Desactualizada

	pueden ser considerados delito informático.		
Gamio (2018, p.25)	El patrimonio está orientado a obtener un fin económico ya que el patrimonio está constituido por bienes, derechos y acciones que se desarrolla de manera personal. En los delitos informáticos La teoría de los Bienes jurídicos afectados son el patrimonio.	El sujeto activo busca lucrar con el desconocimiento de las personas que accede a las plataformas digitales previamente suplantadas por los cibercriminales, razón por la cual corresponde al estado proteger estos Bienes jurídicos los mismos que son supraindividuales	Desactualizada

CONCLUSIÓN: Se puede apreciar que de los nueve autores comparten los mismos criterios que, tomando como punto de partida el supuesto que se deba de uniformar las normas penales para encuadrar esta nueva figura delictiva que busca sacar provecho es decir lucrar económicamente valiéndose del ardid para cometer ilícitos penales.

A continuación, se desarrollará instrumento de guía de revisión del derecho comparado, para responder el objetivo específico 3, el mismo que pretende Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

GUÍA DE ANÁLISIS DEL DERECHO COMPARADO

TÍTULO:

La tipificación del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia.

OBJETIVO ESPECÍFICO 3

Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

País	Asunto a comparar	Norma legal	Cita	Calificación
------	-------------------	-------------	------	--------------

Peru	Aplicación de la Ley de delitos informáticos	La Ley de Delitos Informáticos N.º 30096 y su modificación a través de la Ley 30171	El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa.	Actualizada
Chile	Aplicación y de la ley de delitos informáticos	La ley 21459	El que, causando perjuicio a otro, con la finalidad de obtener un beneficio económico para sí o para un tercero, manipule un sistema informático, mediante la introducción, alteración, daño o supresión de datos informáticos o a través de cualquier interferencia en el funcionamiento de un sistema informático.	Actualizado
Brasil	Ley núm. 12737	Cualquiera que viole las contraseñas u obtenga datos privados y comerciales sin el consentimiento del titular de la cuenta será condenado a tres meses a dos años de prisión y multado.	En Brasil se sanciona a una persona que obtenga datos privados para lucrar económicamente. Ahora en Perú estos delitos son penados de manera más severa y se sanciona con pena privativa de la libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa	Actualizado
Mexico	Artículo 211 bis 1 Código Penal Federal	Al que sin autorización modifique, destruya o provoque pérdida de información contenida en sistemas o equipos de informática protegidos por algún mecanismo de seguridad, se le impondrán de seis meses a dos años de prisión y multado	En nuestro país se sanciona este tipo de conducta con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días multa, mientras que en México es de 6 meses a dos años.	Actualizada

Colombia	Ley de delitos Ley 1273	El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.	En el país de Colombia quien sin orden judicial vulnere un sistema informático será reprimido por 36 a 72 meses en Perú es no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa.	Actualizado
----------	----------------------------	---	--	-------------

ANEXO 5

matriz de categorización

TÍTULO: “La tipificación del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia.”

Categorías	Definición	Subcategorías	Definición	Técnica e instrumento	Procedimientos
PHISHING	Según Herrero (2021), el Phishing es un delito nuevo que merece una tipificación idónea para erradicar la alta incidencia de estos delitos. Para Ortiz (2019) señala que estos delitos se perpetran en la esfera tecnológica, y corresponde a los estados buscar la reducción de los índices de criminalidad, empleando para ello los mecanismos jurídicos necesarios para imputar responsabilidad penal a las entidades financieras	Normativa legal	La Ley de Delitos Informáticos N.º 30096 y su modificación a través de la Ley 30171 no contemplan el surgimiento del phishing, situación que pone en riesgo a la ciudadanía al no estar reguladas estas modalidades ilícitas en el actual marco legal peruano.	Técnica: La entrevista y Instrumento: Guía de entrevista Técnica: análisis documental Instrumento: Guía de análisis normativo legal	Estas técnicas e instrumentos de investigación permitirán responder al objetivo específico 1 y 2
		Doctrina	Cabrera (2017) señala que la Teoría constitucionalista, respecto al delito informático, se encuentra asentada básicamente en la protección constitucional de bienes jurídicos que se encuentran protegidos por la constitución política del estado	Técnica: La entrevista y Instrumento: Guía de entrevista Técnica: análisis documental Instrumento: Guía de análisis doctrinario	
Sistema penal peruano		Derecho comparado	Matute (2017), señala que, debido al aumento del phishing, Ecuador se ha ido adaptando a las nuevas conductas delictivas que se realizan en el espacio digital (p.125).	Técnica: La entrevista y Instrumento: Guía de entrevista Técnica: análisis documental Instrumento: Guía de análisis del derecho comparado	Estas técnicas e instrumentos de investigación permitirán responder al objetivo



GUÍA DE ENTREVISTA

TÍTULO:

"Actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024"

Entrevistado: Guillermo Lloren Perez
Cargo: ABOGADO Institución: PRIVADO

OBJETIVO ESPECÍFICO 1

Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

Preguntas:

1. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?
En efecto, nuestro cuerpo legal no contempla la figura legal del phishing, por ende a la hora de perseguir este delito no existe una correcta imputación de esta nueva modalidad delictiva.
2. Desde su experiencia, ud. cree que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas?
Si, debido principalmente no hay una interpretación normativa, por ende hay vacíos legales para el correcto funcionamiento legal, por ende no hay una contextualización idónea.

OBJETIVO ESPECÍFICO 2

Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024



3. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto?

Doctrinariamente existe poca información respecto al phishing informático en nuestro país, razón por la cual para recurrir a Fuente de Información Doctrinaria se tiene que acudir a información extranjera.

4. Desde su experiencia, ud. cree La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano es desactualizada?

NO existe una norma legal vigente que nos permita tener una información de carácter legal vigente, la norma sobre phishing no está regulada en nuestro sistema legal Peruano.

OBJETIVO ESPECÍFICO 3

Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

5. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?

La Regulación Comparada nos permite tener una visión amplia de como se imputan estos ilícitos, dado que nos señala los actos preparatorios para la consumación de esta delitos.

GUILLEMO
LLEREN PEREZ Firma
ABOGADO
REG. CAL 95241

GUÍA DE ENTREVISTA

TÍTULO:

"Actualidad jurídica del phishing en el sistema penal peruano, para la
lucha contra la ciberdelincuencia, 2024"

Entrevistado: Hubert Dante Gómez Basilio

Cargo: especialista en derecho penal

Institución: privado

OBJETIVO ESPECÍFICO 1

Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

Preguntas:

1. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?

En nuestro marco normativo no está tipificado tipificado la figura legal del phishing, por lo tanto, en el momento de perseguir este delito no va existir una adecuada norma para poder ser juzgada.

2. Desde su experiencia, Ud. cree que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas.

Si, ya que no hay una interpretación normativa correcta, es por ello que existen los vacíos legales para su correcto uso legal, y es así que no hay un correcto entendimiento de esta nueva modalidad.

OBJETIVO ESPECÍFICO 2

Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024



3. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto?

De acuerdo a la normativa existe una mínima información clara sobre el phishing en nuestro país, es por ello se recurre siempre a fuentes extranjeras.

4. Desde su experiencia, ud. cree La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano es desactualizada.

No existe dentro de nuestro marco normativa una información legal vigente que nos va a permitir una información sobre el phishing, por una sencilla razón que no esta regulado en nuestro marco normativo.

OBJETIVO ESPECÍFICO 3

Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

5. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?

La regulación comparada nos va a permitir una amplia información de estos delitos y los marcos normativos extranjeras que ya están regulados nos va visualizar de como deben ser juzgados estos delitos.


ROBERT DANIEL
GÓMEZ BASILIO
ABOGADO
REG. CAL 28468

Firma

ANEXO 3

GUÍA DE ENTREVISTA

TÍTULO

"Actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024"

Entrevistado: *Julian Obregon 2017*

Cargo: *Abogado*

Institución: *Defensoría Pública*

OBJETIVO ESPECÍFICO 1

Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

Preguntas:

1. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?

en la actualidad no, ya que con la última modificatoria de la ley de delitos informáticos en su art. 5 ya está regulado.

2. Desde su experiencia, Ud. cree que La actualidad jurídica phishing en el sistema penal peruano, ¿desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas?

Considero que no, ya que los verbos rectoros son rectoros son claros, además que el tipo penal situaciones como de manera deliberada e ilegítima

OBJETIVO ESPECÍFICO 2

Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

3. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto?

Considero que si, ya que la doctrina nacional existe poca informaciones de los delitos informacion y mas aun que a la fecha ya tiene modificaciones y este resultado.

4. Desde su experiencia, ud. cree La actualidad jurídica phishing en el sistema penal peruano, ¿desde el aspecto doctrinario en el sistema penal peruano es desactualizada?


Considero que si, ya que la realidad en la que vivimos en el Perú a cambiado y los nuevos sociales es que al modificar las normas penales la doctrina se ve desactualizada por mayor tratamiento sobre estos delitos.

OBJETIVO ESPECÍFICO 3

Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

5. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?

Considero que si, ya que en otros países la mayoría de modificaciones van acorde a la jurisprudencia y los delitos informáticos como el phishing.


Judith B. Obregón Isidro
ABOGADA
C.A.L. N° 71270

ANEXO 3
GUÍA DE ENTREVISTA

TÍTULO:

"Actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024"

Entrevistado: Maira Manzanilla Torres

Cargo: Agobago

Institución: Manzanilla y Asociados

OBJETIVO ESPECÍFICO 1

Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

Preguntas:

1. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?

Es saber que nuestro cuerpo legal no contiene la figura que es phishing es así que en el momento castigan esta modalidad no hay una correcta imputación de esta manera delictiva

2. Desde su experiencia, Ud. cree que La actualidad jurídica phishing en el sistema penal peruano, ¿desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas?

Sí, por la razón que no hay una interpretación correcta la cual vale decir que hay vacíos legales para su correcta interpretación y por lo cual no hay una contextualización idónea

OBJETIVO ESPECÍFICO 2

Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

3. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto?

En nuestra doctrina existe una delimitada información y es por esta razón recurrir a información doctrinaria extranjera para su fácil entendimiento.

4. Desde su experiencia, ud. cree La actualidad jurídica phishing en el sistema penal peruano, ¿desde el aspecto doctrinario en el sistema penal peruano es desactualizada?

En nuestra jurisprudencia no hay norma legal que nos brinde una información legal, la norma sobre el phishing no está regulada en nuestro sistema legal peruano.

OBJETIVO ESPECÍFICO 3

Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

5. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?

La regulación comparada nos dará detallada y nos va permitir una visión amplia de como sancionados imputados estos ilícitos penales, en diferentes países el phishing ya esta regulado lo que facilita el juzamiento y prevención del delito.


DAYRA MERIBETH
MANZANILLA TORRES
ABOGADA
REG. CAL. 86333

Firma



GUÍA DE ENTREVISTA

TÍTULO:

"Actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024"

Entrevistado: Sandra Vilchez Alvarado
Cargo: Abogada Institución: Independiente

OBJETIVO ESPECÍFICO 1

Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

Preguntas:

1. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?

Existen vacíos legales y que a la fecha no hay una regulación de la norma penal respecto al phishing como nueva modalidad delictiva.

2. Desde su experiencia, ud. cree que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas?

Exacto al encuadramiento y bajamiento que se le da en la actualidad es de fraude informático. Sin embargo el phishing va más allá que ese solo aspecto jurídico.



OBJETIVO ESPECÍFICO 2

Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

3. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto?

No hay doctrina que defina el Phishing, desde el aspecto doctrinario lo que existe es una visión general sobre este delito (IAFomef.co)

4. Desde su experiencia, ud. cree La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano es desactualizada?

completamente es un delito o modalidad que está en constante auge dada la celeridad en la que se da no se imputa correctamente este tipo de delitos.

OBJETIVO ESPECÍFICO 3

Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

5. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?

El abordaje que se le da no es el idóneo por ende merece una regulación necesaria en la que se define si es un tipo o modalidad (o) elemental para considerarlo delito menor.

GUÍA DE ENTREVISTA

TÍTULO:

"Actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024"

Entrevistado: GUSTAVO CASTILLO MARTINEZ

Cargo:ABOGADO INDEPENDIENTE Institución: PRIVADO

GRADO: Magister en Derecho penal y Procesal penal

OBJETIVO ESPECÍFICO 1

Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

Preguntas:

1. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?

Nuestro marco normativo no cuenta con la regulación adecuada, es por eso en el momento en que va ser juzgado este delito no existe una correcta imputación de modalidades delictivas.

2. Desde su experiencia, ud. cree que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas.

Si, debido a que no está una correcta interpretación adecuada de esta modalidad, es así que hay vacíos legales por lo cual no va a ver un correcto conocimiento sobre ella.

OBJETIVO ESPECÍFICO 2

Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

3. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto?

En nuestro marco legal existe poca información respecto a esta modalidad que es phishing, es así que siempre se va acudir a doctrinas extranjeras, donde que estas tificadas y reguladas dentro de su marco legal.

4. Desde su experiencia, ud. cree La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano es desactualizada.

No existe una norma legal contemplada que nos facilite información idónea, es así que no esta normada dentro de nuestro sistema legal peruano.

OBJETIVO ESPECÍFICO 3

Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

5. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto del derecho comparado está regulado de manera muy general?

Tomando, como base el derecho comparado podemos ver las falencias en nuestra norma penal, en diferentes países el delito de phishing ya se encuentra tipificado en su norma penal lo que facilita su juzgamiento y prevención del mismo. En el caso concreto, México tiene penal de cárcel para aquellos que accedan a la información contenida en sistemas o equipos informáticos del sistema financiero los que tiene protección a través de mecanismos que son vulnerados por los delincuentes


GUSTAVO
CASTILLO MARTINEZ
ABOGADO
REG. CAL. 88365

ANEXO 3

GUÍA DE ENTREVISTA

TÍTULO:

"Actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024"

Entrevistado: Alberto A. Guerra Palaez

Cargo: Abogado.

Institución: Guerra A Asociados

OBJETIVO ESPECÍFICO 1

Explicar desde el aspecto normativo legal es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024.

Preguntas:

1. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto normativo legal en el sistema penal peruano, tiene vacíos legales?

Definitivamente no, nuestro marco normativo no menciona la figura delictiva del phishing y eso que no haya una correcta imputación

2. Desde su experiencia, Ud. cree que La actualidad jurídica phishing en el sistema penal peruano, ¿desde el aspecto normativo legal en el sistema penal peruano invita a interpretaciones descontextualizadas?

Sí, debido que no hay interpretación clara de la norma por eso se dice que hay vacíos legales para su correcta imputación

OBJETIVO ESPECÍFICO 2

Explicar desde el aspecto doctrinario es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

3. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano, desde el aspecto doctrinario en el sistema penal peruano, es obsoleto?

Doctrinariamente la información sobre el phishing es escasa en nuestro país y por ello que se recurre a la doctrina

4. Desde su experiencia, ud. cree La actualidad jurídica phishing en el sistema penal peruano, ¿desde el aspecto doctrinario en el sistema penal peruano es desactualizada?

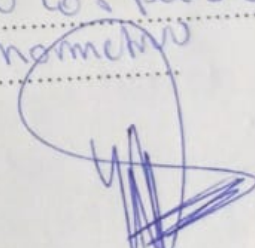

De acuerdo a nuestra actualidad jurídica no hay norma legal vigente que no permita tener una información de carácter eficaz por eso se dice que el phishing no está regulado en ningún ámbito legal peruano.

OBJETIVO ESPECÍFICO 3

Explicar desde el derecho comparado es la actualidad jurídica del phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia, 2024

5. Ud. considera que La actualidad jurídica phishing en el sistema penal peruano desde el aspecto del derecho comparado está regulado de manera muy general?

La regulación comparada nos ayuda tener una amplia información de como los países que están regulados en su marco normativo




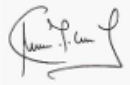


 Elbert A. Guerra Pelaez
ABOGADO
CAL: 43929

Firma

ANEXO N° 3: Informe para proyectos exentos de revisión
Informe de revisión de proyectos de investigación del Comité de Ética en Investigación de la Facultad de Derecho y Humanidades

El que suscribe, presidente del Comité de Ética en Investigación de la Escuela de Derecho, deja constancia que el proyecto de investigación titulado: “La tipificación de phishing en el sistema penal peruano, para la lucha contra la ciberdelincuencia”, presentado por el/los autor (es): PERALTA HUAMÁN, ALEX JAIME, queda exento de revisión de acuerdo a la verificación realizada por: Dr. Matienzo Mendoza, Jhon Elionel; Dr. Lugo Denis, Dayron; Dra. Zevallos Loyaga, María Eugenia; Dr. Castañeda Mendez, Juan Alberto; Mg. Fuentes Vásquez, Jhon Cristian; Mg. Palomino Gonzales Lutgarda de acuerdo a la comunicación remitida el día 14 de noviembre con el informe que sustenta la exención de revisión del proyecto, por lo cual se determina que la continuidad para la ejecución del proyecto de investigación cuenta con un dictamen favorable.

Trujillo, 16 de noviembre del 2023

	Cargo	DNI N.º	Firma
Dr. Lugo Denis, Dayron	Presidente	C.E. N° 001911323	
Dra. Zevallos Loyaga María Eugenia	Secretaria	D.N.I. 18190178	
Dr. Castañeda Méndez. Juan Alberto	Miembro 3	D.N.I. 73894422	
Mg. Fuentes Vásquez, Jhon C	Miembro 4	D.N.I. 44979795	
Mg. Palomino Gonzales, Lutgarda	Miembro 5	D.N.I. 22422843	
Dr. Matienzo Mendoza Jhon Elionel	Miembro 6	D.N.I. 40233048	