FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Inseguridad en el delito informático a través de la modalidad del *smishing* y *phishing*

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTOR:

Taipe Huaman, Diego Saul (orcid.org/0000-0003-4852-0390)

ASESOR:

Mtro. Guerra Campos, Jefferson Williams (orcid.org/0000-0003-0158-7248)

LÍNEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia, liderazgo y ciudadanía

LIMA - PERÚ

2023

Dedicatoria

A mi familia, por estar en todo este transcurso de mi carrera, aconsejándome y guiándome desde un inicio por su apoyo incondicional.

Agradecimiento

A mis padres y mis hermanos por siempre aconsejarme en las decisiones que me he encaminado y los consejos brindados, asimismo agradecer a mis maestros por compartir sus conocimientos en todo el transcurso de mi carrera.

Declaratoria de autenticidad del asesor

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, GUERRA CAMPOS JEFFERSON WILLIAMS, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, asesor de Tesis Completa titulada: "Inseguridad en el delito informático a través de la modalidad del smishing y phishing", cuyo autor es TAIPE HUAMAN DIEGO SAUL, constato que la investigación tiene un índice de similitud de 9.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis Completa 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, 08 de Diciembre del 2023

Apellidos y Nombres del Asesor:	**Firma**
JEFFERSON WILLIAMS GUERRA CAMPOS **DNI:** 71012547 **ORCID:** 0000-0003-0158-7248	Firmado electrónicamente por: JGUERRACA el 21-12-2023 12:44:48

Código documento Trilce: TRI - 0688918

INVESTIGA UCV

Declaratoria de originalidad del autor

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Originalidad del Autor

Yo, TAIPE HUAMAN DIEGO SAUL estudiante de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA ESTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis Completa titulada: "Inseguridad en el delito informático a través de la modalidad del smishing y phishing", es de mi autoría, por lo tanto, declaro que la Tesis Completa:

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**
DIEGO SAUL TAIPE HUAMAN **DNI:** 47330318 **ORCID:** 0000-0003-4852-0390	Firmado electrónicamente por: DTAIPEH el 08-12-2023 20:03:10

Código documento Trilce: TRI - 0688919

INVESTIGA UCV

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

Resumen

El trabajo de investigación, tuvo como objetivo general en determinar los criterios que se deben de considerar para tipificar la modalidad del *smishing* y *phishing* en la Ley de delitos informáticos, en cuanto a la metodología se realizó con un enfoque cualitativo, de tipo básico y con un diseño fenomenológico, asimismo la técnica utilizada en el desarrollo de la investigación fue la entrevista y el instrumento se realizó con la guía de entrevista, por lo cual, se contó con 5 participantes de las cuales cumplieron con los criterios de inclusión y exclusión (abogados y/o trabajadores del ministerio público especializado en materia de derecho penal y procesal penal, tener más de 5 años como profesionales y residir en Lima). Por lo cual se concluyó que los criterios que se deben de considerar para tipificar la modalidad del smishing y phishing es el acceso no autorizado, la manipulación, el contenido engañoso, la suplantación de identidad y el inducir al error para que realice un acto de disposición en perjuicio propio, por lo cual, tipificando esta modalidad en la legislación peruana tendría un impacto positivo, garantizando un debido proceso y una debida aplicación de la pena. Asimismo, la conducta principal de estas modalidades, es la obtención de datos personal o financiera, para posteriormente obtener un beneficio económico.

Palabras clave: Delito informático, *smishing*, *phishing*, patrimonio.

Abstract

The general objective of the research work was to determine the criteria that must be considered to classify the modality of smishing and phishing in the computer crime law. Regarding the methodology, it was carried out with a qualitative approach, of a basic type and with a phenomenological design, likewise the technique used in the development of the research was the interview and the instrument was carried out with the interview guide, therefore, there were 5 participants of whom met the inclusion and exclusion criteria (lawyers and/or public ministry workers specialized in criminal law and criminal procedure, have more than 5 years as professionals and reside in Lima). Therefore, it was concluded that the criteria that must be considered to classify the modality of smishing and phishing are unauthorized access, manipulation, misleading content, identity theft and misleading people to carry out an act of disposal. to one's own detriment, therefore, typifying this modality in Peruvian legislation would have a positive impact, guaranteeing due process and due application of the penalty. Likewise, the main conduct of these modalities is the obtaining of personal or financial data, to later obtain an economic benefit.

Keywords: Computer crime, smishing, phishing, heritage.

I. INTRODUCCIÓN

La tecnología ha servido de gran aporte al desarrollo de la sociedad, otorgando facilidades para que las personas sean más eficaces en sus actividades diarias, por ejemplo, en el transporte, la educación, la salud, el trabajo, la comunicación y otras actividades sociales en general (Rojas & Yepes, 2021). Una de las facilidades que a brindado el avance tecnológico, es en la forma como las personas se puedan comunicar por medio de un teléfono inteligente, computador, tablet o laptop, por lo cual se comunican a través de los mensajes (SMS), correos electrónicos y/o mediate diferentes redes sociales. No obstante, estos aportes tecnológicos han traído problemas sociales. (Ospina & Sanabria, 2020),

Estas actividades han generado que personas facinerosas ejecuten actividades al perjuicio de una colectividad de personas que utilizan estos medios tecnológicos, creando nuevos *modus operandi* para delinquir (Santacruz & Hermoza, 2019). Por ello, la legislación peruana ha tomado medidas legislativas para contrarrestar dichos ilícitos cibernéticos mediante la Ley n.° 30096 (Guevara, 2022). Por otro lado, mientras la tecnología va avanzando, van apareciendo nuevas modalidades para delinquir mediante el uso de la tecnología (Urpeque, 2019). Por lo cual, la Ley contra el delito informático no tipifica de forma expresa estas nuevas modalidades que son el *smishing y phishing*.

Por ende, en los últimos años, la legislación peruana ha tenido cambios para combatir el ciberdelito incorporando por primera vez el delito informático mediante el Decreto Legislativo n.° 681, el 14 de octubre del 1991, que regula la utilización de tecnologías en asunto de archivo de información o documentos (Paredes, 2013). Siendo así, que la última actualización del delito cibernético se lleva a cabo con la Ley n.° 30171 que modificó la Ley n.° 30096 del delito informático del 17 de febrero del 2014 (Huaman, 2020). Por lo cual, aun teniendo estas últimas modificaciones, existen deficiencias en la legislación peruana para tipificar dicha conducta (Arellano & Galindo, 2022; Vilca, 2018; Carrillo & Montenegro, 2018).

Este accionar delictivo va cambiando de la misma forma que los medios tecnológicos van evolucionando, apareciendo nuevas formas para cometer este accionar delictivo que está relacionado con los medios tecnológicos (Villón et al., 2019). Asimismo, esto delimita la realización de una buena tipificación idónea de acuerdo a la realidad social. Por lo que esto conlleva que la justicia peruana no realiza una adecuada tipificación para detectar a tiempo quiénes son los que cometieron este ilícito. Por lo cual el Estado tiene que invertir en medios tecnológicos que ayuden a detectar a los que cometieron este accionar delictivo y a una adecuada norma que tipifique la modalidad delictiva (Ventura, 2021).

Además, en la legislación existen vacíos en la tipificación de los delitos informáticos, como es en el art. 8 de la Ley de Delitos Informáticos, menciona que el fraude informático contra el patrimonio, en la cual no tipifica el *modus operandi* de la modalidad del *smishing y phishing*. Toda vez que esta modalidad induce al engaño previo, siendo que hace referencia al delito de estafa (Mayer & Oliver, 2020). Esto podría ser en los casos que el agraviado o el sujeto pasivo manipula su mismo datos o programas para transferir dinero de su cuenta bancaria a otra cuenta bancaria, esto es realizado sin la manipulación del sujeto activo, por lo cual no calzaba en lo que estipula el art. 8 de la Ley n.° 30096. Asimismo, esta Ley no se encuentra establecida y acorde a la realidad social, siendo necesario modificar e incorporar ciertos elementos que tipifiquen estas modalidades en dicha Ley antes mencionado.

Al respecto, Zorrilla (2018) mencionó que la modificación de la Ley n.° 30096 son cambios que se realizó para contrarrestar los delitos realizados por los medios tecnológicos, aunque resulte deficiente y esto no cuadra adecuadamente en los tipos penales, intenta cesar los medios y la forma de delinquir. Asimismo, Chiluisa (2021) indicó que el delito informático abarca a todos los ciudadanos del país y en base a las Leyes que son específicas para combatir la ciberdelincuencia, han sido consideradas insuficientes por un delito que se renueva y va avanzando con la tecnología, generando vacíos legales, por consiguiente, en vez de combatir la delincuencia, la entorpece.

El presente estudio tiene como pregunta general lo siguiente: ¿Cuáles son los criterios que se deben de considerar para tipificar la modalidad del *smishing*

y *phishing* en la Ley de delitos informáticos?; Asimismo, tiene como preguntas específicas: (a) ¿Cuáles son los beneficios de tipificar la modalidad del *smishing* y *phishing* en la Ley de delitos informáticos? Y (b) ¿Cuáles son las conductas delictivas del *smishing* y *phishing* en la jurisdicción peruana?

Por lo cual, la presente investigación se justifica, debido que estas modalidades ilícitas que son en *smishing y phishing* no se encuentran tipificadas en la Ley de delitos informáticos. Por lo tanto, las autoridades tienen la dificultad para tipificar estas conductas delictivas a efecto de no tener una buena tipificación de estas nuevas modalidades que va apareciendo a consecuencia del avance tecnológico, por otra parte, estos delitos han tenido un crecimiento exponencial en estos últimos años. (Ventura, 2021)

En este sentido, los representantes del Ministerio de Justicia y Derechos Humanos (MINJUSDH, 2022) mencionaron que en el 2019 se registró un total de 7108 denuncias; en el 2020, se registró 8897 denuncias; y, en el 2021, se registró 14671 denuncias sobre delitos informáticos, teniendo un crecimiento exponencial en el accionar de este delito. Asimismo, es menester mencionar que la investigación contiene algunas limitaciones como, por ejemplo, obtener libros especializados en delitos informáticos actuales y obtener carpetas fiscales sobre el delito informático.

En esa misma línea, el objetivo general del desarrollo de la investigación es determinar los criterios que se deben de considerar para tipificar la modalidad del *smishing* y *phishing* en la Ley de delitos informáticos, mientras que, los objetivos específicos planteados son: a) Indicar los beneficios de tipificar la modalidad del *smishing* y *phishing* en la Ley de delitos informáticos, y b) Analizar las conductas delictivas del *smishing* y *phishing* en la jurisdicción peruana.

II. MARCO TEÓRICO

De acuerdo a los antecedentes internacionales, en el estudio realizado por Garzon & Cuero (2022), tuvieron como objetivo de investigación en la asimilación que deberían de tener los delitos informáticos en relación con los tipos penales que ha sido clasificado como delito de impacto en Colombia. Por lo cual, se utilizó la metodología descriptiva con un enfoque analítico cuantitativo, mediante un registro estadístico del Sistema de Información Estadístico Delictivo y Contravencional de la Policía Nacional de Colombia. Donde concluyó que los delitos informáticos han tenido un crecimiento sucesivo en Colombia, Siendo que, estos delitos a no ser del tipo penal común, necesitan formas y métodos especiales para su realización por lo cual el sujeto activo tiene conocimiento especializado en informática o programación.

Trávez (2018), en su trabajo de su investigación tuvo como objetivo determinar la vulneración de los derechos por la falta de tipificación de las nuevas conductas delictivas a través de la tecnología. El trabajo de investigación tuvo un enfoque mixto, cuantitativo y cualitativo, teniendo resultados estadísticos y también profundiza al análisis de cada resultado obtenido de acuerdo a su marco teórico. Asimismo, se llegó a la conclusión que, en la legislación de Ecuador, aun teniendo una normativa penal que regula el delito informático, esto dificulta aplicar las normas existentes, ya que no se tiene una debida tipificación o el tipo no se encuentra en el nuevo código orgánico integral penal. Por consiguiente, existe vacíos legales en el derecho informático, a consecuencia de los nuevos delitos informáticos con características específicas.

Por lo cual, Utreras (2017), en su desarrollo de investigación indicó que su objetivo general fue en determinar la relación entre la estafa tradicional y el fraude informático. Teniendo como metodología un enfoque cualitativo, la cual tiene la necesidad de tipificar este accionar en la Ley chilena, asimismo se ha llevado a cabo una revisión normativa, jurisprudencial y doctrinaria. Teniendo como conclusión que los tipos penales vigentes no son idóneos para sancionar el fraude informático, siendo que la conducta es atípica, en la cual se debería de tipificar este accionar para tutelar el patrimonio de las personas, ya que, el fraude

informático desborda el alcance de tipos penales como el hurto, la estafa y los delitos de la Ley n.º 19.223.

Como antecedentes nacionales de la presente investigación, sobre la inseguridad informática, se tiene a Camacho & Figueroa (2022), en su trabajo de investigación considero como objetivo general en analizar la intervención del estado para tratar lo delitos informáticos contra el patrimonio. Empleando como método de investigación el enfoque cualitativo, basado en la normativa de la Ley n.º 30171 en su artículo 8. En lo cual, concluyó que la regulación de la norma es poco eficiente, a consecuencia del avance tecnológico, siendo que esta Ley no se encuentra regulada a la realidad social. Lo cual amerita por parte del estado peruano la actualización de la Ley de Delito Informático.

Para Ramos & Salvador (2022), en su trabajo de investigación propusieron en su objetivo, en fundamentar la regulación de las nuevas modalidades del delito informático en la Ley n.º 30096. Teniendo un enfoque cualitativo, en lo cual participio 5 fiscales provinciales de la ciudad de Huaraz. Asimismo, concluyeron que las modalidades de *smishing, phishing y vishing* deben de ser incorporadas en la Ley de Delitos Informáticos como conductas específicas, con el fin de ser sancionado, ya que muchos de estas modalidades suelen ser archivadas por no tener un tipo penal adecuado.

Asimismo, para Nazario & Villanueva (2022), en su tesis tuvieron como objetivo general aplicar una actualización de la legislación para una eficiente persecución y sanción penal del delito de fraude informático en la modalidad del *phishing*. Esta investigación se realizó mediante un enfoque mixto (cuantitativo y cualitativo). Concluyeron que la legislación peruana requiere una adecuada actualización en la Ley de delitos informáticos, a consecuencias de la nueva modalidad de *phishing*, por lo cual en la actualidad no existe una adecuada tipificación penal, quedando impune estos actos ilícitos por esta nueva modalidad

En las siguientes líneas se desarrollará las bases teóricas de las categorías: la Ley del delito informático y la tipificación de las modalidades de *smishing* y *phishing*

Este delito informático ha tenido relevancia a partir del año 1990, por la cual se creó el Decreto Legislativo n.º 681 el 14 de octubre del 1991, que regula el uso de la tecnología en materia de archivo de información o documento (Espinoza, 2020). De esta misma manera la tecnología ha estado evolucionando de forma precipitada. El uso de la tecnología ha favorecido a una mejor calidad de vida, como en la comunicación, a través de celulares inteligentes, dándonos la facilidad de realizar diferentes actividades virtualmente, como depósito interbancario, comunicarnos por las diferentes redes sociales, los mensajes de texto, videollamadas, etc. (Becerra, 2022).

Por lo cual, no solo ha traído en la legislación peruana beneficios, también ha conllevado que personas utilicen estos medios tecnológicos para delinquir, por lo cual, en el 2013 se creó la Ley de Delitos informáticos, Ley n.º 30096, con fecha 21 de octubre del 2013. Posteriormente se realizaron modificaciones de acuerdo a la Ley n.º 30171 con fecha 17 de febrero del 2014. (Huaman, 2020).

Asimismo, en el 2020 el delito informático tuvo un gran incremento a razón del estado de emergencia que nuestro estado implementó a razón del Covid-19 (Garzon & Cuero 2022, Camacho & Figueroa 2022). Donde se llegó a visualizar con mayor frecuencia las diferentes modalidades para cometer el fraude cibernético. Estos son mediane la modalidad del *smishing y phishing*, modalidades con la cual se han estado cometiendo delitos contra el patrimonio en la sociedad. Asimismo, en la legislación no está debidamente tipificando este accionar, existiendo deficiencia en nuestra legislación sobre los delitos informáticos. (Arellano & Galindo, 2022; Carrillo & Montenegro, 2018)

De acuerdo a, López (2020), que mencionó que la tipificación nos permite diferenciar las figuras delictivas o los tipos penales, en esta misma forma, para indicar que una conducta sea delictiva, tendrá como requisitos ser típica, esto se refiere que la acción u omisión debe de cuadrar en uno de los tipos penales, en su parte objetiva y subjetiva descrito en Ley. De lo antes mencionado, si el comportamiento o la conducta no cuadra en ningún tipo penal, estará ante una conducta atípica (Ataoglu, 2020). De acuerdo a lo mencionado el delito informático en la legislación se rige con la Ley n.º 30096, que tiene como finalidad, en prevenir y sancionar las conductas antijurídicas que son ejecutados

a través de la tecnología de la información, teniendo como última modificación de fecha 17 de febrero del 2014 mediante Ley n.º 30171 publicado el 10 de marzo del 2014 donde cuenta con 12 artículos hasta la actualidad.

El bien jurídico tutelado en el derecho penal, se trata de resguardar los bienes jurídicos fundamentales de una persona y de la sociedad, que tiene como objetivo mantener el orden social., como es el patrimonio, la vida, salud, la privacidad, la libertad, etc. En el ciberdelito se tiene como bien jurídico tutelado la información, como principal bien jurídico protegido, pero también son afectados otros conjuntos de bienes debido a la conducta típica, de esta forma bienes ser un delito pluriofensivo (Vinelli, 2021). Asimismo, Acurio (s.f.) indicó que el tipo de conductas criminal en el delito cibernético es pluriofensivo, porque no solo se afecta un solo bien jurídico, sino a varios bienes jurídicos, por ejemplo, el patrimonio, la confiabilidad de los datos, la seguridad de comunicaciones informáticas etc.

En el delito cibernético se tiene a dos sujetos procesales, uno es el sujeto activo y el otro el sujeto pasivo. El sujeto activo es la persona que realiza una conducta típica y el sujeto pasivo es el usuario, esto podría ser una persona natural o jurídica que es titular del bien jurídico afectado. De acuerdo a Espinoza (2022) el sujeto activo es el individuo que mediante el empleo de la tecnología tenga un provecho ilegal mediante, el diseño, alteración, supresión, borrado, deterioro, clona datos informáticos, intercambia datos para un beneficio propio o de terceros. Por lo cual, el sujeto activo tiene conocimiento en el manejo del sistema informático, y, el sujeto pasivo es usuario titular de los datos informáticos transgredido. (Parada & Errecaborde, 2018).

En el delito cibernético ha surgido en la actualidad diferentes formas de cometer el delito de fraude informático por parte del sujeto activo, una de esta modalidad es el *phishing*, en lo cual, el sujeto activo envía correos electrónicos fraudulentos haciéndose pasar por una empresa, persona o servicio de confianza para que el usuario brinde su información personal y bancaria. Asimismo, Nazario y Villanueva (2022) indicaron que el *phishing* tiene como modalidad la captación de datos a través de correos electrónicos, que simulan diferentes identidades de empresas conocidas para generar confianza.

Solicitando datos de su tarjeta por diversos motivos, como promoción, problemas de seguridad, depósito bancario internacional o nacional, bloqueos, etc. Esto tiene como finalidad la captación del dinero o crédito de la tarjeta bancaria.

Por otro lado, se tiene que la modalidad del es el *smishing* que es similar al *phishing,* a diferencia en que esta modalidad consiste en enviar al sujeto pasivo (víctima) un SMS o al WhatsApp mensajes con contenidos maliciosos que contengan enlaces web, aplicaciones e interfaz que perjudica a cualquier usuario (Rodríguez, 2020). Para Adriano (2017) indicó que el *smishing* es la forma más práctica de infectar un teléfono móvil, con la autorización inocente del usuario. Asimismo, los atacantes se hacen pasar por una institución conocida o una persona real, para hacerle creer al usuario que los mensajes son reales para obtener información personal. (Montalbán, 2023)

Estas dos modalidades antes descritas son de tipo fraude, en lo cual, tiene como finalidad común obtener información personal del usuario para obtener sus datos virtuales y realizar acciones ilícitas. Por lo cual, en el *phishing* o *smishing* se consuma el delito mediante un perjuicio a su patrimonio cuando el sujeto activo sustrae el dinero de su cuenta bancaria sin el consentimiento de la víctima. (García, 2021).

En el sistema legislativo, en la Ley n.° 30096, Ley del delito informático, su artículo 8 menciona el delito informático contra el patrimonio, mediante el fraude informático. En lo cual, tuvo su última modificación por la Ley n.° 30171 de fecha 10 de marzo del 2014. Asimismo, la modalidad del *smishing* y *phishing* tiene como una de sus características, en vulnerar el bien jurídico del sujeto pasivo, que es su información y su patrimonio, cuando el sujeto activo tiene la información personal de la víctima, este realiza una transferencia bancaria o adquiere bienes, como también adquiere servicios al nombre de la víctima, generando un perjuicio patrimonial. (Ramos & Salvador, 2022)

Debido a que estas conductas ilícitas no son tipificadas de manera explícita en el delito informático contra el patrimonio, estos casos llegan a ser archivados por no contar con un tipo penal adecuado que describa de forma correcta la modalidad del *smishing y phishing.*

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

3.1.1. Tipo de investigación

Según el propósito de la investigación, se procura tener información relevante, por lo cual, la investigación es del tipo básico. Esto tiene como fin producir y buscar nuevos conocimientos (Gallardo, 2017). En efecto, esto es esencial para el beneficio social a largo plazo para otras investigaciones futuras (Ñaupa et al., 2018).

3.1.2. Diseño de investigación

Consiguientemente, el enfoque de investigación es cualitativo pues tiene como concepto recopilar la opinión de la población escogida mediante las entrevistas. Según Sánchez (2019), el enfoque cualitativo se sustenta en evidencias que son obtenidas mediante la descripción profunda, de acuerdo a la percepción del fenómeno.

Asimismo, se ha aplicado el diseño de investigación fenomenológico. Según Sánchez et al. (2020), este método busca entender lo que expresa una persona, en base a todo lo que ha experimentado en una determinada manera. Por último, el nivel de investigación es el exploratorio, que consiste en abordar temas poco estudiados. Según Amaiquema et al. (2019). Indicó que el diseño exploratorio se realiza cuando no se ha abordado, a gran escala, el tema a realizar, la cual tiene como propósito entender el problema y su entorno.

3.2 Categorías, subcategorías y matriz de categorización

Según Sánchez et al. (2022), las categorías permiten precisar la información que se desea recoger para la investigación. Asimismo, en esta investigación cuenta con 2 categorías principales que son la Ley de delitos informáticos, n.° 30096 y la tipificación de las conductas delictivas del *smishing* y *phishing*.

Tabla 1

Matriz de categorización

Categorías	Sub-categorías	Criterio n.° 1	Criterio n.° 2
Ley de delitos informáticos Ley n.° 30096	delitos informáticos contra el patrimonio	Fraude	Patrimonio
La tipificación de las conductas delictivas del *Smishing* y *Phishing*	Criterio para tipificar el tipo penal	Engaño	Técnicas de manipulación
	El medio empleado en cometer el ilícito penal.	MSM	Correo electrónico

3.3 Escenario de estudio

El desarrollo de la investigación se está realizando conforme a cada categoría, teniendo como entrevistados a abogados y fiscales especialista en el derecho penal perteneciente a la ciudad de Lima, el estudio del desarrollo de la investigación se realizó por la falta de la tipificación de las nuevas modalidades del ciberdelito, que son el *smishing* y *phishing* en el sistema jurídico peruano. Según Escudero & Cortés (2017), el escenario consiste en detalles históricos, geográficos y temporales, ayudando al investigador y lector a tener una imagen sobre el contexto social y natural del lugar donde se realiza el estudio.

3.4 Participantes

La investigación se ha desarrollado con la colaboración de 5 especialistas, quienes son profesionales y especialistas en la materia del derecho penal y procesal penal, conformados por abogados y/o trabajadores del Ministerio Publico del departamento de Lima quienes brindaron su colaboración voluntariamente; y 2 expertos en la materia del derecho penal que validaron la guía de entrevista. Asimismo, se han analizado diversas publicaciones de autores nacionales e internacionales referente al tema de investigación. A continuación, se mostrarán los criterios que se realizaron para la clasificación de los especialistas y expertos.

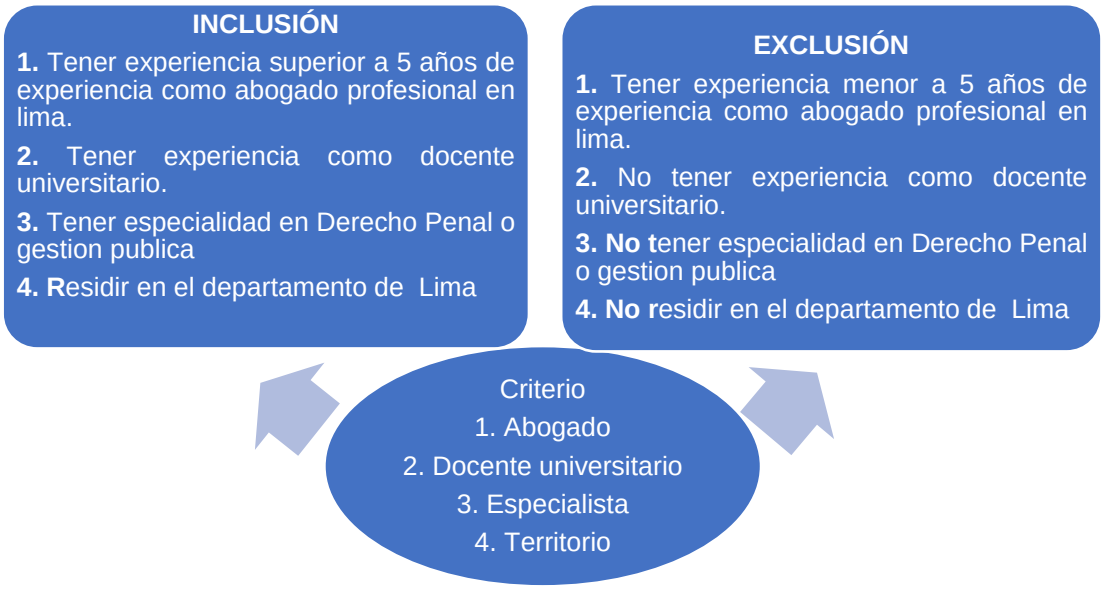
Figura 1

Criterios de inclusión y exclusión de los participantes.

En la selección de los participantes se tomaron los criterios de selección de la figura 1.

Figura 2

Criterios de inclusión y exclusión de los expertos.



En la selección de los expertos se tomaron los criterios de selección de la figura 2.

3.5 Técnicas e instrumentos de recolección de datos

Según Ñaupa et al. (2018) la recolección de datos es un proceso que tiene como fin reunir datos específicos proporcionados por personas con la finalidad de analizarlo, para luego responder las preguntas de la investigación, esto es de acuerdo al enfoque cualitativo.

Al especto, Gallardo (2017) preciso que la técnica y el instrumento sirve para que el investigador obtenga información relevante para el desarrollo de su investigación. Por lo cual, este proyecto se realizó con la técnica de entrevista a profundidad, la cual se formuló 9 preguntas a cada participante utilizando el instrumento de guía de entrevista, donde los participantes respondieron según sus conocimientos profesionales.

Por lo cual, se ha desarrollado la ficha de resumen de técnicas de instrumentos, de acuerdo a la siguiente tabla 2

Tabla 2

Ficha de resumen de la técnica instrumental.

Aspectos clave		**Instrumento**
Técnica	Objetivo	Guía de instrumento
Entrevista	Determinar cuáles son los elementos que se deben de considerar para tipificar la modalidad del smishing y phishing en la Ley de delitos informáticos.	Profundidad
Origen de procedencia		Propio
Contenido		09 ítems
Enfoque		Cualitativo
Fiabilidad y validez	Criterio de Jueces	1.- Molocho Vega Luis Edison 2.- Morales Olivera David
Muestra de aplicación		Profesionales del derecho que se encuentren habilitados y especializados en derecho penal con una trayectoria de 5 años a más de experiencia.

3.6 Procedimiento

En el desarrollo de la investigación se empleó la recolección de información, mediante documentos referente al tema a investigar de fuentes confiables como Renati, Scopus, Proquest, Redalyc, Scielo y entre otras fuentes, toda la información es sobre la Ley de delitos informáticos y la modalidad del *smishing* y *phishing*. Después de esto se utilizó los instrumentos metodológicos de la entrevista a profundidad, mismos que fueron previamente validados por los expertos, quienes confirmaron la fiabilidad, viabilidad y confiabilidad, para obtener un buen resultado para el objetivo de la investigación.

En la entrevista a profundidad se contó con 5 especialistas, entre abogados y fiscales expertos en la materia del derecho penal, con experiencia mayor a 5 años. Por la cual, se utilizó la guía de entrevista a profundidad. La entrevista se realizó presencialmente, lo cual se dispuso con un tiempo máximo de 20 minutos, utilizando una grabadora de inicio a fin de la entrevista, para luego analizar la información obtenida por los entrevistados para poder desarrollar los resultados y discusiones. Finalmente, se desarrolló las conclusiones y recomendaciones.

Asimismo, para el avance de la presente tesis, se realizaron gastos, tales como la compra de hojas, fotocopias, impresiones, USB, pasajes para la movilidad, entre otros.

3.7 Rigor científico

En el desarrollo del trabajo de investigación se elaboró con rigor científico. Al respecto. Hernández & Mendoza (2018) indicaron que en el rigor del estudio cualitativo se utilizan ciertos criterios que son la dependencia, credibilidad, transferibilidad y confirmabilidad, por lo cual, la presente investigación se aplicaron los criterios antes ya señalados para que tengan un buen rigor científico, teniendo concordancia los objetivos y preguntas específicas con el título establecido.

La dependencia o consistencia hace referencia a la estabilidad de datos, esto quiere decir que exista coherencia entre el título y las preguntas objetivas asegurando la credibilidad de los datos. (Arias & Giraldo, 2011)

Asimismo, Escudero & Cortez (2018) mencionaron que la credibilidad está relacionada con la riqueza y calidad de los datos e información que se llega a obtener en el desarrollo de la investigación. Estos datos obtenidos de los resultados de los participantes que están en relacionados al fenómeno de investigación.

En la transferibilidad consiste en poder aplicar los resultados del desarrollo de la investigación a otros, dichos resultados servirán para comparar con otros estudios de acuerdo al contexto que se aplique, y por último el criterio de la confirmabilidad, permite conocer el trabajo desarrollado por el investigador, teniendo en consideración cuales ha sido sus limitaciones y alcances del fenómeno estudiado (Espinoza, 2020). Siendo que esto permita que otros investigadores apliquen estos alcances y limitaciones a futuras investigaciones del fenómeno estudiado.

3.8 Método de análisis de datos

En el desarrollo de la investigación se ha utilizado el método hermenéutico en el análisis de datos, teniendo como fin interpretar y analizar los materiales que se han llevado a cabo en el desarrollo de la investigación, tales como artículos, revistas, tesis, grabaciones que se realizaron a los entrevistados. Según Pérez y Nieto (2022), mencionaron que la hermenéutica es la facultad de interpretar la información a analizar. Asimismo, para Rojas & Arroyo (2020), la hermenéutica es una actividad interpretativa que permite un mejor entendimiento en las diferentes etapas de la investigación. Para Ramos (2018) menciono que conocer los métodos nos brinda un mejor significado a los textos normativos.

3.9 Aspectos éticos

En el proceso del presente trabajo no se han manipulado o falsificado los datos. Según Inguillay et al. (2019), el aspecto ético en los trabajos de investigación demuestra que los trabajos a realizar son libres de plagio. Por lo

tanto, esta investigación se ha elaborado conforme a las normas que dicta la Universidad César Vallejo de acuerdo a la resolución de Consejo Universitario n.° 0470-2022/UCV que aprobó la actualización del Código de Ética en investigación, asimismo, se han citado a diferentes autores de libros, tesis, revistas y artículos, siguiendo las normas la American Psychological Association, APA en su 7ma edición. Que sirve para poder reconocer las ideas de los autores y citarlas correspondientemente para no vulnerar el derecho de autor, por lo cual se siguen los requisitos formales.

Por lo cual, en el desarrollo de la investigación se aplicó el principio ético de la beneficencia. Para Zerón (2019), este principio hace referencia a mejorar la calidad de vida y promover el bienestar de los sujetos en la investigación. Lo cual, este principio tiene como fin en no generar daño y contribuir con el bienestar de los sujetos.

IV. RESULTADOS Y DISCUSIÓN

Pregunta n.° 1: En su opinión, ¿Cuáles son los vacíos legales informáticos a consecuencia de la nueva modalidad del *smishing* y *phishing*?

Tabla 3

Pregunta n.° 1: repuestas

Entrevistados	Repuesta de la pregunta n.° 1
C.F.S.C.	De acuerdo a nuestra Ley de delitos informáticos, estas modalidades están tipificadas de forma general en nuestra legislación, siendo que no hay un artículo que defina la modalidad *smishing* y *phishing*.
V.R.S.B.	La imposibilidad de tipificar estas modalidades incluye de gran parte la evolución de la tecnología, por lo cual dificulta su persecución y saber la verdadera identidad de los delincuentes para establecer la responsabilidad legal.
D.Z.C	En la modalidad del smishing y phishing en nuestra Ley de delitos informáticos, no aborda definiciones específicas, lo cual dificulta la interpretación y aplicación de la Ley en casos específicos.
J.L.A.R.	El smishing y phishing es una forma de fraude informático que no está debidamente tipificado en la Ley especial de los delitos informáticos, en lo cual no se describe el accionar de estas modalidades, imposibilitando la debida tipificación por parte del ministerio público. Por lo cual, en casos especifico se llega a tipificar como un delito de estafa o como suplantación de identidad de acuerdo al artículo 9 de la Ley n.° 30096.
L.O.A.	Teniendo en cuenta que estas nuevas modalidades cibernéticas no están específicamente tipificadas en nuestra legislación, tenemos que tener en cuenta que no solo basta de tener una debida tipificación, tenemos que considerar que la autoridad judicial no puede tipificar debidamente este delito por la falta de medios probatorios idóneos, por consiguiente, estos delitos son archivados en su mayoría por no ubicar quienes son los responsables.

Tabla 4

Pregunta n.° 1: análisis

Convergencia	Divergencia	Interpretación
Los entrevistados de manera unánime indicaron que los vacíos legales se deben a consecuencia que nuestra Ley de delito informático en los delitos contra el patrimonio, solo tipifican en forma general, no especificando dicha modalidad.	Algunos entrevistados Indicaron que a veces estos delitos no se llegan a tipificar por la dificultad de obtener evidencias fehacientes, por lo cual, se llegan a tipifiquen por otros delitos, como suplantación de identidad o delito de estafa.	Los entrevistados indican que nuestra Ley de delitos informáticos no tipifica estas modalidades, por lo cual, nuestra Ley actual solo tipifica delitos contra el patrimonio de forma general, asimismo algunos entrevistados indicaron que no solo basta tipificar estas modalidades para dejar de tener este vacío legal, esto también se debe a consecuencia que en la actualidad es dificultoso obtener evidencias idóneas que identifique quienes son los responsables.

Pregunta n.° 2: ¿Considera usted que identificando los criterios que tipifiquen la modalidad del *smishing* y *phishing* sería un disuasivo para que los delincuentes no empleen esta modalidad?

Tabla 5

Pregunta n.° 2: repuestas

Entrevistados	Repuesta de la pregunta n.° 1
C.F.S.C.	Teniendo una tipificación idónea de estas modalidades en nuestra legislación, los delincuentes cibernéticos tendrán claro de las consecuencias legales de su accionar.
V.R.S.B.	Si sería un gran disuasivo a que otros no comentan este delito, si está debidamente tipificado ya que ayudaría a procesar a los delincuentes de forma más efectiva y así se tendría una condena de acuerdo a su accionar delictivo.
D.Z.C	Lo delincuentes, por más que tipifiquen un accionar delictivo, no van a dejar de cometer el phishing y smishing, siendo que ellos son van a crear nuevas tácticas para eludir la medida legal que se implementa.
J.L.A.R.	Si, por lo cual esto tendría un gran impacto para reducir y combatir la ciberdelincuencia, ya que se contaría con una buena base legal para presentar cargos hacia los delincuentes que utilizan la tecnología,
L.O.A.	Si sería un gran disuasivo en nuestra legislación, pero no sería suficiente para que estos delitos disminuyan, ya que la tecnología avanza a pasos a agigantados, por lo cual se crean nuevas formas de delinquir mediante estas modalidades, por lo cual estos delincuentes empleen esta modalidad, pero con diferente estrategia. Los cual los servidores públicos tendrían que estar en constante capacitación.

Tabla 6

Pregunta n.° 2: análisis

Convergencia	Divergencia	Interpretación
Los entrevistados coincidieron que sería un disuasivo para que lo delincuentes no empleen esta modalidad, ya que se contaría con una buena base legal especifica y se tendrían claro cuáles serían las consecuencias legales de su accionar.	Algunos entrevistados mencionaron que también se tendría que incorporar nuevas herramientas digitales para combatir este delito con mayor eficacia y estar a al mismo avance tecnológico, capacitándose constantemente.	Los entrevistados señalan que tipificando estas modalidades sería un disuasivo para que los delincuentes no empleen esta modalidad, siendo que se tendría claro cuáles serían las consecuencias legales y se tendría una condena de acuerdo a su accionar delictivo, pero no solo bastaría una buena tipificación, también se tendría que implementar nuevas herramientas (software) y estar constantemente capacitados. Ya que los delincuentes crearan nuevas formas de eludir las mediades legales que se implementan.

Pregunta n.° 3: ¿Considera usted que la tipificación del *smishing* y *phishing* reduciría considerablemente el índice de los delitos informáticos contra el patrimonio?

Tabla 7

Pregunta n.° 3: repuestas

Entrevistados	Repuesta de la pregunta n.° 1
C.F.S.C.	Si se reduciría en gran parte, pero se tiene que tener en cuenta que esta modalidad no solo afecta al patrimonio, sino a la seguridad informática. Por lo cual, si se quiere reducir el índice de delitos informáticos se tendría que fortalecer la seguridad informática, empleando estrategias para prevenir que terceros sean perjudicados mediante estas modalidades.
V.R.S.B.	Claro que si reduciría, teniendo una buena tipificación reduciría este ilícito, ya que nuestra Ley de delito informáticos desde el 2014 hasta la actualidad no ha tenido una actualización. Siendo este delito que se comenten mediante la tecnología, ha surgido nuevas formas para delinquir.
D.Z.C	Toda tipificación de un nuevo delito o modalidad ayuda a que exista seguridad jurídica y así estos delitos tenga poca repercusión a que se configure,
J.L.A.R.	Si considero que reduciría el índice de los delitos informáticos, pero no solo es tipificar este accionar y que esta conducta deje de perpetuarse. Lo que se tendría que realizar para que baje el índice de este delito es generar campaña de información de estas nuevas modalidades.
L.O.A.	Toda tipificación de un hecho delictivo, siempre reducirá el índice delictivo, ya que se establecen las consecuencias legales que tendrían que afrontar quienes llegaran a cometer este acto ilícito.

Tabla 8

Pregunta n.° 3: análisis

Convergencia	Divergencia	Interpretación
Todos los entrevistaron señalan que si reduciría el índice del delito informático contra el patrimonio,	Algunos entrevistados resalta que aparte de la tipificación se debería de implementar estrategias para fortalecer la seguridad informática y realizar campañas informáticas de estas modalidades.	Los entrevistados coinciden que si reduciría en gran parte el delito informático contra el patrimonio, mencionando que toda tipificación de un hecho delictivo ayuda que exista seguridad jurídica, la cual establece las consecuencias legales que tendrán que afrontar los delincuentes cibernéticos, asimismo indicaron algunos entrevistados que no solo basta tipificar un delito, también es realizar campañas informáticas de estas nuevas modalidades y emplear estrategias para prevenir que terceros se han perjudicados.

Pregunta n.° 4: En su opinión, ¿Considera usted que tipificando la modalidad del *smishing* y *phishing* garantizaría la seguridad jurídica?

Tabla 9

Pregunta n.° 4: repuestas

Entrevistados	Repuesta de la pregunta n.° 1
C.F.S.C.	Si generaría seguridad jurídica, por lo cual, teniendo una tipificación clara y precisa, esto ayudaría a las autoridades y fiscales poder aplicar correctamente la Ley en los delitos informáticos.
V.R.S.B.	Considero que sí, porque esto garantizaría que todos los procesos sean justo, como también se fijaría una buena aplicación de la pena, ponderando el daño causado, lo cual tendríamos una mejor sanción penal y civil.
D.Z.C	Si considero, por que garantizaría la protección los derechos de los agraviados y garantizando la proporcionalidad de la pena que se establezca al imputado.
J.L.A.R.	Estas modalidades no solo vulneran la seguridad informática de un estado, sino el sistema financiero es afectado, por lo cual, tipificando estas modalidades ayudaría de gran medida en garantizar la seguridad jurídica, ya que los delitos informáticos es un delito pluriofensivo.
L.O.A.	Si garantizaría la seguridad jurídica, ya que no habría impunidad cuando se cometa los delitos a través de estas modalidades, garantizando la protección del derecho del agraviado.

Tabla 10

Pregunta n.° 4: análisis

Convergencia	Divergencia	Interpretación
Los entrevistado de forma uniforme indicaron que si garantizaría la seguridad jurídica, por lo cual garantizaría la correcta aplicación de la pena, lo cual garantizaría la proporcionalidad de la pena, siendo este un delito pluriofensivo.	Algunos entrevistados indicaron que tipificando habría un proceso más justo, protegiendo el derecho del agraviado.	Los entrevistados coinciden que si garantizaría la seguridad pública, porque habría una buena aplicación de la pena, siendo este un delito pluriofensivo, asimismo garantizaría el derecho a un debido proceso, protegiendo el derecho del imputado y del agraviado, por lo cual se aplicaría una sanción penal y civil acorde al daño ocasionado mediante estas modalidades que tiene como fin obtener un bien patrimonial.

Pregunta n.° 5: En su opinión, ¿Cree usted que tipificando la modalidad del *smishing* y *phishing* habría menos carpetas fiscales archivadas por la falta de una buena tipificación?

Tabla 11

Pregunta n.° 5: repuestas

Entrevistados	Repuesta de la pregunta n.° 1
C.F.S.C.	Si tendría un impacto positivo, porque se podría procesar los delitos de manera justa y oportuna, ya que se podría cuadrar el delito en un tipo penal, siendo que las carpetas no se archiven por falta de una buena tipificación.
V.R.S.B.	En la actualidad las carpetas se archivan por falta de los medios de convicción, no es solo tipificar el delito, sino tener los medios probatorios tecnológicos que nos ayuden a seguir con la investigación del delito.
D.Z.C	Si ayudaría en reducir el archivamiento de las carpetas fiscales, pero tipificado este accionar no basta, se requieren recursos adicionales para la persecución de estos delitos, uno de esto es la identificación de los imputados.
J.L.A.R.	Teniendo una norma clara que llene esos vacíos legales por la falta de una debida tipificación, reduciría el archivamiento de las carpetas fiscales, ya que hay casos que se archivan porque la Ley no especifica este accionar y la forma como induce al error al agraviado para obtener sus bienes patrimoniales.
L.O.A.	Si reduciría en poca medida, porque en la mayoría de estas denuncias no se llega a formalizar la denuncia penal a consecuencias de los medios probatoria, en donde no se puede identificar a los imputados del delito informático.

Tabla 12

Pregunta n.° 5: análisis

Convergencia	Divergencia	Interpretación
Todos los entrevistados coincidieron que si habría reduciría el archivamiento de las carpetas fiscales, a consecuencia que se podría cuadrar el tipo penal de estas nuevas modalidades.	Algunos entrevistaron indicaron que estos delitos a veces son archivados por falta de medio de prueba de convicción, donde se identifiquen a los imputados.	Los entrevistados indicaron que si reduciría el archivamiento de las carpetas fiscales, esto es a consecuencia de que el accionar delictivo, mediante estas nuevas modalidades, se podrían cuadrar este accionar en un tipo penal que especifiquen la modalidad del phishing y smishing, por lo cual se llegaría a formalizar la denuncia penal y no se archivaría la carpeta fiscal. Asimismo, otros entrevistados indicaron que no es solo tipificar estas modalidades, sino también contar con los medios probatorios para identificar a los imputados para seguir con la investigación del delito.

Pregunta n.° 6: ¿Considera usted que tipificando la modalidad delictiva del *phishing* y *smishing* ayudaría a proteger futuros delitos subyacentes?

Tabla 13

Pregunta n.° 6: repuestas

Entrevistados	Repuesta de la pregunta n.° 1
C.F.S.C.	Si considero que ayudaría proteger ciertos delitos subyacentes, como la suplantación de identidad, o como obtener información no autorizada.
V.R.S.B.	Si ayudaría proteger futuros delitos, por lo cual esta modalidad al momento de obtener los datos robados, pueden causar daños financieros, suplantación de identidad, extorsión, entre otros delitos.
D.Z.C	La modalidad del phishing y smishing son acciones delictivas que tiene como propósito cometer otros delitos subyacentes que pueden ser el fraude informático, suplantación de identidad, espionaje, entre otros delitos.
J.L.A.R.	Si protegerían, ya que tipificado esta modalidad ayudaría a prevenir y combatir este delito informático y prevendría delitos que se llegan a realizar a consecuencia de haber obtener estos datos informáticos por emplear estas modalidades.
L.O.A.	Siendo el phishing y smishing una técnica para obtener información y posteriormente cometer diferentes delitos como el fraude informático y como también suplantación de identidad y otros delitos, si considero que ayudaría a que se realice estos delitos subyacentes,

Tabla 14

Pregunta n.° 6: análisis

Convergencia	Divergencia	Interpretación
Los entrevistados indicaron que tipificando protegería delitos subyacentes, como el delito suplantación de identidad, espionaje, extorsión, venta de datos informáticos entre otros delitos.,	Algunos entrevistados indicaron que el fin de esta modalidad es obtener información para luego realizar la sustracción de su patrimonio, causando daños financieros.	Los entrevistaron mencionaron que tipificando estas modalidades tendría un gran impacto en proteger y prevenir delitos subyacentes como la suplantación de identidad, espionaje, seguridad informática, extorsión, entre otros. Asimismo, indicaron que el fin de estas modalidades es en sustraer información para luego sustraer el patrimonio del agraviado, siendo que esta modalidad ataca a más de un bien jurídicamente protegido. Por lo cual, viene ser un delito pluriofensivo

Pregunta n.° 7: ¿Considera que las personas que comenten estos actos delictivos mediante la tecnología, son profesionales en la tecnología de la información y las comunicaciones (TIC)?

Tabla 15

Pregunta n.° 7: repuestas

Entrevistados	Repuesta de la pregunta n.° 1
C.F.S.C.	No considero que todos los que comente este delito sean profesionales, siendo que, hay algunos que solo cuenta con conocimiento técnicos y otros que solo se encarga de obtener el dinero de las cuentas bancarias.
V.R.S.B.	Estas modalidades en su mayoría son cometidos por personas que tienen conocimientos básicos. No especialmente tienes que ser profesional en la TIC. Ya que ellos pueden comprar programas diseñados para cometer estos actos delictivos.
D.Z.C	No generalizaría en el aspecto de que sean todos profesionales de la tecnología. Un ejemplo claro, es en las organizaciones criminales informáticas, lo cual, cada uno tiene una función específica sin ser profesional de la TIC.
J.L.A.R.	Profesionales en la TIC son los que crean los programas o herramientas para cometes este accionar, creando software sofisticados para que ellos lo utilicen o como también vender estos programas a persona con poco conocimiento en la TIC.
L.O.A.	No todos los ciberdelincuentes son profesionales de la TIC, ya que muchos de ellos pueden comprar estos programas previamente creados para realizar estos delitos que es el phishing o smishing.

Tabla 16

Pregunta n.° 7: análisis

Convergencia	Divergencia	Interpretación
Los entrevistados de manera unánime indicaron que no necesariamente los ciberdelincuentes tienen que ser profesionales de la TIC.	Algunos entrevistaron indicaron algunos ciberdelincuentes, solo cuenta con conocimiento básico, siendo que solo obtienen estos programas mediante el mercado negro.	Los entrevistado de forma unánime expresaron que los que comenten estos delitos informáticos, no necesariamente tienen que ser profesionales de la TIC, los que son profesionales en su mayoría crean software y una vez que cometen su ilícito y haber obtenido su objetivo, venden estos programas para que personas con conocimiento básico utilizan estos programas. Asimismo, en las organizaciones criminales de ciberdelincuencia, hay delincuentes que solo tienen conocimiento básico en la tecnología.

Pregunta n.° 8: ¿Cree usted que el accionar de los delincuentes que cometen estos ilícitos están relacionados con una organización criminal?

Tabla 17

Pregunta n.° 8: repuestas

Entrevistados	Repuesta de la pregunta n.° 1
C.F.S.C.	Siendo esto un delito informático puede estar relacionados con una organización internacional. A si mismo hay una planificación por medio en como captar a sus potenciales víctimas.
V.R.S.B.	En su mayoría sí, porque los delitos informáticos requieren de otras personas, por ejemplo, quienes son los que reciben el dinero por transferencia bancaria, el que manda mensaje de texto o mensajes a través de correos electrónicos y quienes desarrollan las páginas web que suplantaran la identidad de una empresa reconocida.
D.Z.C	Claro que pueden estar relacionado con una organización criminal, pero en la práctica es laboriosos identificarlos, por lo cual, solo se llega a tener a un presunto sospechoso.
J.L.A.R.	Los medios empleados, la planificación de obtener la información de las potenciales víctimas de su cuenta bancaria, si están relacionados con una organización criminal. Pero es un desafío constante identificar a esta organización criminal.
L.O.A.	No todos los casos pueden estar relacionado con una organización criminal, esto influye bastante en hallar a los responsables y cumplir con los elementos para considerar una organización criminal.

Tabla 18

Pregunta n.° 8: análisis

Convergencia	Divergencia	Interpretación
Los entrevistados mencionaron que los delincuentes que comenten este ilícito necesariamente no son organizaciones criminales.	Algunos entrevistaron mencionaron que los delincuentes que cometen estos delitos mediante una organización criminal, es más tedioso identificar a los autores, siendo que algunos operan fuera de la jurisdicción peruana, siendo un esto desafío constantes en identificar estas organizaciones criminales.	Los entrevistados indicaron que el accionar de los delincuentes cibernéticos no necesariamente tiene que estar involucrado en una organización criminal, toda vez que solo lo llevan a cometer en compañía de otra persona, siendo que no cuadraría en la tipificación de una organización criminal. Asimismo, indicaron que las organizaciones criminales en su mayoría operan fuera de la jurisdicción peruana, siendo más dificultoso la persecución y en encontrar a los responsables, por lo cual es tedioso identificar una organización criminal, a consecuencia que están debidamente organizadas.

Pregunta n.° 9: En su opinión, ¿Considera que este acto de delinquir lo pueden realizar fuera de la jurisdicción peruana, para así evitar su identidad y así permanecer en el anonimato?

Tabla 19

Pregunta n.° 9: repuestas

Entrevistados	Repuesta de la pregunta n.° 1
C.F.S.C.	Las personas que comenten este delito procuran no ser identificados por las autoridades. Y algunas personas puede accionar fuera de otro país para así su persecución por parte de la autoridad sea más complicado para identificarlo y así permanecer en el anonimato.
V.R.S.B.	Si considero, ya que ellos comenten este delito mediante el internet, en donde ellos podrían realizar este accionar estando en otro país, con el fin que pueda ser identificado.
D.Z.C	Estos sujetos, utilizan estos medios tecnológicos para que no puedan ser identificados y en su parte lo realizan en países que no estén suscrito en el Convenio de Budapest. Para permanecer en el anonimato y seguir delinquiendo.
J.L.A.R.	Si considero, ya que el internet es un espacio abierto en donde las personas interactúan con personas de diferente país. Siendo esto una gran ventaja para los delincuentes no pueda ser reconocidos.
L.O.A.	Los delincuentes pueden realizar estos delitos en diferentes partes del mundo, a consecuencia de esta problemática nuestro estado peruano se suscribió al convenio de Budapest para tener una cooperación con los otros países para poder trabajar en conjunto y así identificar al delincuente y este no permanezca en el anonimato.

Tabla 20

Pregunta n.° 9: análisis

Convergencia	Divergencia	Interpretación
Los entrevistados mencionaron que los delincuentes cibernéticos utilizan el internet para ocultar su identidad, permaneciendo en el anonimato y así evitar la persecución de estos tipos de delitos. Siendo que algunos lo realizan fuera de la jurisdicción de un estado.	Algunos entrevistados refirieron que realizan este acto delictivo en diferente parte del mundo, siendo el internet un medio que puede ser utilizado en diferente lugar de cualquier país.	Los entrevistaron de manera unánime indicaron que, si se puede realizar este delito estando en otro país, toda vez que el internet es un medio que cualquier persona puede interactuar con cualquier individuo estando en diferente parte del mundo, asimismo dificultando ser identificado, para seguir delinquiendo, es por esta causa que el Perú se incorporó al convenio de Budapest en el 2019 para cooperar en la lucha contra la ciberdelincuencia.

Discusión

Objetivo General: Determinar los criterios que se deben de considerar para tipificar la modalidad del *smishing* y *phishing* en la Ley de delitos informáticos.

En la Ley especial de delitos informáticos, en el Art. 8 que habla de los delitos contra el patrimonio sobre fraude informático, lo cual solo tipifica los delitos contra el patrimonio de forma general y no especifica la modalidad del *smishing* y *phishing*, estas modalidades en mucho de los casos se realizan para obtener ganancias financieras. Lo cual deberían estar específicamente tipificado en los delitos informáticos contra el patrimonio.

Asimismo, teniendo estos criterios establecidos, los delincuentes cibernéticos tendrán en claro cuáles serían las consecuencias legales que tendrían que afrontar, por lo tanto, sería un disuasivo para que ellos no realicen esta acción mediante el *phishing* y *smishing,* de igual manera, se tendría una condena de acuerdo a su accionar delictivo.

En esa línea, Ventura (2019) indicó que a consecuencia de la pandemia del covid-19 quedó en evidencia la necesidad de clasificar algunos criterios en la Ley de delitos informáticos, esto a raíz de las nuevas modalidades de fraude informático, asimismo, estas que son el *phishing* y *smishing* implica en la obtención indebida de los activos financieros intangible.

Por lo tanto, los criterios que se debe de tener en cuenta es el medio que emplean estas modalidades, el propósito, el engaño, la suplantación de identidad, el método y el perjuicio patrimonial.

De esta forma, el ciberdelincuente emplea esta modalidad para obtener información personal con el fin de obtener un beneficio patrimonial ilícito. Teniendo como criterio la obtención de información personal mediante los diferentes medios tecnológicos.

Además, Hidalgo & Solano (2021) mencionaron que la Ley n.° 30096 pretende subsumir el delito informático contra el patrimonio solo mencionando los verbos rectores, por lo cual no tipifica esta modalidad delictiva, que ocasiona una inseguridad jurídica. Siendo que esta modalidad implica engañar, haciendo creer a la persona que está ante una identidad confiable. Tiendo como elemento clave el engaño y fraude.

Teniendo una debida tipificación en la legislación reduciría este ilícito y garantizaría la seguridad jurídica, pero también el Estado tendría que fortalecer la seguridad informática. Asimismo, teniendo en cuenta que la Ley de delitos informáticos tuvo su primera modificatoria el 10 de marzo del 2014 y hasta la actualidad no ha tenido una actualización, por lo cual esta Ley no es acorde a la realidad social, teniendo en cuenta que este delito se realiza por medios tecnológicos y estas mismas han evolucionado, por lo cual se han creados nuevas formas de delinquir por estos medios tecnológicos.

Para Nazario & Villanueva (2022) sostuvieron que la debida tipificación del *phishing* nos permite una persecución penal eficiente para luego obtener una sanción acorde al acto ilícito, generando una correcta persecución y sanción penal.

Objetivo específico 1: Indicar los beneficios de tipificar la modalidad del *smishing* y *phishing* en la Ley de delitos informáticos.

Tipificando estas modalidades garantizaría la seguridad jurídica, siendo que el *phishing* y *smishing* tiene una conducta delictiva que afecta a varios bienes jurídicos protegidos, lo cual esta modalidad es pluriofensiva, asimismo garantizaría el derecho a un debido proceso, protegiendo el derecho del imputado y del agraviado, por lo cual se aplicaría una sanción penal y civil acorde al daño ocasionado.

Asimismo, Acurio (s.f) indico que para que exista una adecuada protección a los sistemas informáticos, se debe de relacionar la seguridad informática como la seguridad legal, por lo cual la seguridad normativa proviene de los principios de legalidad y la seguridad jurídica, Por lo tanto, la seguridad jurídica en los delitos informáticos se debe usarse para impedir los ataques ya

sean fuera del sistema informático y dentro del mismo. Incorporando políticas claras y precisas para una debida protección.

Teniendo una norma clara que llene esos vacíos legales reduciría el archivamiento de las carpetas fiscales, por lo cual se podría cuadrar este accionar en un tipo penal que especifiquen la modalidad del phishing y smishing, asimismo se llegaría a formalizar la denuncia penal y no se realizaría el sobreseimiento de manera definitiva en un proceso penal. Por otra parte, no solo es tipificar esta modalidad, sino también contar con los medios probatorios para identificar a los imputados.

Para, Cabrera (2020) concluyo que los delitos informáticos en el cercado de Cajamarca se archivaron por la falta de la conducta ilícita, al no cumplir con los elementos de tipicidad y también por la falta de individualización del imputado. Ramos & Salvador (2022) indicaron que los delitos contra el patrimonio a través del phishing son tipificados como estafa simple o agravada.

Por último, otro de los beneficios es que ayudaría a proteger y prevenir delitos subyacentes como la extorsión, el tráfico ilegal de datos, la suplantación de identidad, estafa, entre otros. Por lo cual, tipificando estas nuevas formas de cometer este ilícito se prevendrían a que no se comentan otros delitos subyacentes. Trávez (2018) sostuvo que, tipificando las nuevas conductas delictivas, brindaría mayor seguridad a los usuarios o cibernautas, teniendo como beneficiarios directos a toda persona que son víctimas por utilizar estos medios tecnológicos de comunicación y como beneficiarios indirectos serían los terceros que son afectados a consecuencia de la información obtenida del beneficiario directo.

Objetivo específico 2: Analizar las conductas delictivas del *smishing* y *phishing* en nuestra jurisdicción peruana.

Sobre las conductas de los delincuentes cibernéticos, no es necesariamente ser un profesional en la tecnología de la información y las comunicaciones (TIC) para cometer este ilícito, solo basta con tener conocimientos básicos en informática, por lo cual, algunos delincuentes solo

compran software o programas sofisticados en la *drak web* (web oscura) para poder cometer este ilícito.

Teniendo en cuenta a Urpeque (2019) indico que el sujeto activo en los delitos informáticos, puede ser cualquier persona, este con solo conocimiento y habilidades básicas en la informática, siendo esto un delito dominio. Por ende, no se tiene que generalizar que todos lo que comenten este accionar sean profesionales de la TIC, de esta forma se puede indicar que, en una organización criminal de ciberdelincuentes no todos son profesionales, lo cual, cada integrante tiene una función específica.

Los ciberdelincuentes en su mayoría para no ser identificados integran una organización criminal para cometer este ilícito y así la investigación sea más compleja. Pero no es necesario en que conforme una organización criminal para que puedan delinquir y no ser ubicados, de esta forma a veces solo, siendo que por el internet una sola persona puede realizar diferentes funciones a la misma vez.

Asimismo, en el Art. 11 de la Ley n°30096 nos menciona que el juez aumenta la pena hasta un tercio por encima del máximo legal si el delincuente comete cualquier delito que está previsto en la Ley antes mencionada si es integrante de una organización criminal.

Estos actos por medio de la tecnología, también lo realizan fuera de la jurisdicción peruana, con el fin de no ser identificados y así permanecer en el anonimato, dificultando la persecución por parte de nuestro estado, a consecuencia de esta problemática el Perú se suscribió al convenio de Budapest para cooperar con otros países en la lucha contra la ciberdelincuencia el 13 de febrero del 2019. Por lo tanto, Urpeque (2019) se refirió que la actividad criminal por los medios tecnológicos ha rebasado fronteras de competencias jurisdiccionales, danto que el marco normativo ha dado pase a instrumentos supranacionales.

Por lo cual, el instrumento normativo utilizado en estos casos, es el convenio de Budapest que ayuda en la cooperación de la investigación y asistencia mutua para investigar y procesar delitos informáticos.

V. CONCLUSIONES

Primero. Los criterios que se deben de considerar para tipificar la modalidad del *smishing* y *phishing* en el capítulo V de la Ley n.° 30096 es el medio de comunicación, esto puede ser mediante mensaje de texto (SMS) o correos electrónicos, con la intención de obtener un beneficio económico. Esto podría ser el acceso no autorizado, la manipulación, el contenido engañoso, la suplantación de identidad y también el inducir al error para que realice un acto de disposición en perjuicio propio. Por lo tanto, se debería de incorporar en el capítulo V de la Ley de Delitos Informáticos estos criterios para una debida tipificación de estas nuevas modalidades.

Segundo. La tipificación de estas modalidades en la legislación peruana tendría un impacto positivo en la persecución del delito informático contra el patrimonio y a la misma vez generaría seguridad jurídica, garantizando un debido proceso, de la misma forma, se garantizaría una correcta aplicación de la pena. Por lo cual habría menos carpetas archivadas por falta de una correcta tipificación, asimismo, esto beneficiaria a proteger y prevenir delitos subyacentes que se puede realizar a causa del *smishing* y *phishing*.

Tercero. Sobre estas modalidades, la conducta principal, es la obtención de información personal o financiera, para después obtener un beneficio económico, por lo cual, estos actos delictivos lo pueden realizar cualquier persona, por lo cual solo basta tener un conocimiento básico en la informática, razón por la cual estas personas sin ser profesionales de la TIC pueden consiguen en la *drak web* (web oscura) software o herramientas digitales para poder delinquir mediante *smishing* y *phishing*.

Los ciberdelincuentes, en su mayoría, para no ser identificados integran una organización criminal, y en algunos de los casos, lo realizan estando en otro país, con el fin de no ser identificado y así evitar la persecución de tales conductas. De esta misma forma, los que integran una organización criminal no necesariamente son profesionales en la tecnología, teniendo cada uno diferentes habilidades y funciones con el fin de cometer un ilícito.

VI. RECOMENDACIONES

Se sugiere al Poder Legislativo incorporar en el capítulo V de la Ley de Delitos Informáticos el Art. 8-A, donde se tipifique específicamente las modalidades del *phishing* y *smishing*, los cual han sido expuesto en el presente trabajo.

Asimismo, se recomienda que la Ley de delito informático sea analizado cada 3 años para generar futuras adecuaciones o modificaciones a causa de las nuevas modalidades que van surgiendo de acuerdo al avance tecnológico, con el fin, de que no se generen vacíos legales por la falta de una buena tipificación.

.

REFERENCIAS

Acurio. S. (s.f.). Delitos informáticos: generalidades. Recuperado de http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/599

Adriano. J. (27 de agosto del 2017). Cuidado con el “Smishing”. El Norte Retrieved from https://www.proquest.com/newspapers/cuidado-con-el-smishing/docview/1932552815/se-2

Amaiquema, F., Vera, J., & Zumba, I. (2019). Enfoques para la formulación de la hipótesis en la investigación científica. *Revista Conrado*, 15(70), 354-360. Recuperado de http://conrado.ucf.edu.cu/index.php/conrado

Arellano, G. & Galindo, S. (2022). Deficiencias Legislativas en el Tratamiento de la Ley N° 30096, Ley de Delitos Informáticos – Fraude Informático, Lima 2019 – 2021. (Tesis para optar el título profesional de abogado). Universidad Cesar Vallejo. https://hdl.handle.net/20.500.12692/102672

Arias, M. & Giraldo, C. (2011). El rigor científico en la investigación cualitativa. Investigación y Educación en Enfermería, 29(3), 500-514. https://www.redalyc.org/articulo.oa?id=105222406020

Ataoglu, S. (2020). Ilícitos atípicos: una crítica. Ius et Praxis, 26(1), 192-206. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0718-00122020000100192

Becerra, C. (2022). Innovación en pagos digitales en el Perú: Retos al 2030. (Tesis para obtener el grado académico de Magíster en Gestión y Política de la Innovación y la Tecnología). Pontifica Universidad Católica del Perú. https://tesis.pucp.edu.pe/repositorio/handle/20.500.12404/23425

Cabrera, M. (2020). “FUNDAMENTOS JURÍDICOS CONSIDERADOS POR LOS FISCALES PENALES DE CERCADO DE CAJAMARCA PARA ARCHIVAR LAS INVESTIGACIONES DE DELITOS INFORMÁTICOS DURANTE EL PERIODO DEL 2010-2018” (Tesis para optar el título profesional de abogada). Universidad Privada del Norte. https://repositorio.upn.edu.pe/handle/11537/24533

Camacho, J. & Figueroa, G. (2022) Análisis del Artículo 8º de la Ley N.º 30171 de los Delitos Informáticos contra el Patrimonio en el Perú. (Para optar el Título profesional de Abogado). Universidad Cesar Vallejo. https://hdl.handle.net/20.500.12692/94805

Carrillo, C. & Montenegro, A. (2018). La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos. (Para optar el Título profesional de Abogado). Universidad Señor de Sipán. https://hdl.handle.net/20.500.12802/4514

Chiluisa, D. (2016). Los delitos informáticos y los vacíos legales que afectan a los ciudadanos. (Trabajo de titulación previo a la obtención del título de Abogado de los tribunales y juzgados de la república del Ecuador). http://repositorio.ucsg.edu.ec/handle/3317/16501?locale=fr

Cordero, N. (2021) LA CIBERDELINCUENCIA. (Master Universitario en Acceso a la Profesión de Abogado). Universidad de Alcalá. https://ebuah.uah.es/dspace/handle/10017/49563

Escudero, C. & Cortes, L. (2017) Técnicas y métodos cualitativo para la investigación científica. Editorial UTMACH

Espinoza, E. (2020). La investigación cualitativa, una herramienta ética en el ámbito pedagógico. Revista Conrado, 16(75), 103-110. http://scielo.sld.cu/pdf/rc/v16n75/1990-8644-rc-16-75-103.pdf

Espinoza, J. (2020) “APLICACIÓN DE LA MICROFORMA DIGITAL EN LAS JUNTAS GENERALES DE ACCIONISTAS Y DIRECTORIOS NO PRESENCIALES DE LA SOCIEDAD ANÓMIMA CERRADA” (Trabajo de investigación para optar el Grado Académico de Maestro en Derecho Empresarial). Universidad de Lima https://repositorio.ulima.edu.pe/handle/20.500.12724/11712

Espinoza, j. (2022). Factores que inciden en la tipicidad objetiva del delito de fraude informático, ministerio público Chepén, 2022. (tesis para obtener el título profesional de abogado). Universidad Cesar Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/114016

Gallardo, E. (2017) *Metodología de la Investigación. Manual Autoformativo Interactivo*. Universidad Continental. https://repositorio.continental.edu.pe/bitstream/20.500.12394/4278/1/DO_UC_EG_MAI_UC0584_2018.pdf

García, E. (2021). DELITOS CONTRA EL PATRIMONIO ECONÓMICO, EL PHISHING EN COLOMBIA, APROXIMACIÓN CRIMINOLÓGICA. (Tesis o grado para optar el grado de magister de Derecho). Universidad Nacional de Colombia. https://repositorio.unal.edu.co/handle/unal/82270

Garzon, J. & Cuero. K. (2022). Una mirada a la cibercriminalidad en Colombia y su asimilación con los delitos de impacto. *Revista Criminal*. 64(3), 203-313. https://doi.org/10.47741/17943108.373

Gorostidi, J. (2022). Sobre el alcance de los fines de la pena en el fenómeno criminal de la ciberdelincuencia. *Revista chilena de derecho y tecnología*. 11(1) 121-146. file:///C:/Users/PC/Downloads/tapiagorostidi.pdf

Guevara, A. (2022). INFLUENCIA DE LOS DELITOS INFORMATICOS EN EL CONTEXTO DE EMERGENCIA SANITARIA EN LIMA METROPOLITANA, AÑO 2021. (Para optar el Título profesional de Abogado). Universidad Peruana de las Américas. http://repositorio.ulasamericas.edu.pe/handle/upa/1889

Hernández, R., Fernández. C. & baptista, P. (2014) Metodología de la investigación. (6 ed.). McGRAW-HILL

Hidalgo, C. & Solano. G. (2021). “EL PHISHING COMO CONDUCTA DELICTIVA NO REGULADA EN EL ORDENAMIENTO JURIDICO PERUANO. PROPUESTA DE INCORPORACIÓN DEL ARTÍCULO 7-A EN LA LEY DE DELITO INFORMÁTICOS 30096” (Tesis para obtener el título profesional de abogado). Universidad Nacional del Santa. https://repositorio.uns.edu.pe/bitstream/handle/20.500.14278/3849/52376.pdf?sequence=1&isAllowed=y

Huaman, M. (2020). LOS DELITOS INFORMATICOS EN PERÚ Y LA SUSCRIPCIÓN DEL CONVENIO DE BUDAPEST. (Tesis para optar el

título de abogada). Universidad Andina del Cusco. https://hdl.handle.net/20.500.12557/4116

Inguillay, L., Tercero, S., & López, J. (2020). Ética en la investigación científica. *Revista Imaginario Social*, 3(1). https://doi.org/10.31876/is.v3i1.10

López, Y. (2020) LA TEORIA DEL DELITO: revisión crítica del elemento culpabilidad (Tesis de Doctorado) Pontifica Universidad Católica Argentina. https://repositorio.uca.edu.ar/handle/123456789/11122

Marhuenda, S. (2017). Evolución de la criminalidad en España. Sistemas de Información Geográfica (SIG), una aplicación práctica en la localidad de San Fulgencio (Trabajo final de Grado). Universidad Miguel Hernández. http://dspace.umh.es/handle/11000/6960

Mayer, L., & Oliver, G. (2020). El delito de fraude informático: concepto y delimitación. *Revista Chilena De Derecho Y Tecnología*, 9(1), 151–184. https://doi.org/10.5354/0719-2584.2020.57149

Montalbán, E. (13 de mayo del 2023). Advierten sobre nueva modalidad de fraude telefónico: 'smishing'. El Vocero De Puerto Rico https://www.proquest.com/newspapers/advierten-sobre-nueva-modalidad-de-fraude/docview/2813491871/se-2

Nazario, N. & Villanueva, L. (2022). FRAUDE INFORMÁTICO EN LA MODALIDAD DE PHISHING Y LA NECESARIA ACTUALIZACIÓN DE LA LEGISLACIÓN PARA UNA EFICIENTE PERSECUCIÓN Y SANCIÓN PENAL. (Tesis para optar el título profesional de abogado). Universidad Señor de Sipán. https://repositorio.uss.edu.pe/handle/20.500.12802/10002

Novoa, I & Venegas, L. (2022) Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional. (Memoria para optar al grado de Licenciado en Ciencias Jurídicas y Sociales) Universidad de Chile. https://repositorio.uchile.cl/bitstream/handle/2250/176344/Herramientas-

del-convenio-de-Budapest-sobre-ciberdelincuencia-y-su-adecuacion-a-la-legislacion-nacional.pdf?sequence=1&isAllowed=y

Ñaupa, H., Valdivia, Q., Palacios, J & Romero, H. (2018) Metodología de las investigación cuantitativa – cualitativa y Redacción de la tesis, 5a. Edición. Bogotá: Ediciones de la U.

Ospina, M. & Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista criminal*. 62(2) 199-217. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-31082020000200199&lang=es

Parada, R y Errecaborde, J. (2018). *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet*. Buenos Aires: Erreius.

Pérez, J. & Nieto, J. (2022). La narrativa como método de investigación teológica en una epistemología hermenéutica. *Cuestiones Teológicas*, 49(111), 1-19. doi: http://doi.org/10.18566/cueteo.v49n111.a02

Ramos, C. (2018). *CÓMO HACER UNA TESIS DE DERECHO Y NO ENVEJER EN EL INTENTO*. Perú :Lex & Iuris.

Ramos, M. & Salvador, Y (2022). “La regulación de las nuevas modalidades del delito informático en la Ley N° 30096 y su modificatoria, periodo 2020-2021”. (tesis para obtener el título profesional de abogado). Universidad Cesar Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/108873

Rojas, B. & Arroyo, A. (2020). Perspectiva hermenéutica y vigencia de los modelos narrativos para la investigación en ciencias sociales. *Universitas humanística*. 89, ISSN: 0120-4807/2011-2734. Recuperado de: https://doi.org/10.11144/Javeriana.uh89.phvm

Rojas, J. & Yepes, J. (2021) Panorama de riesgo por el uso de la tecnología en América Latina. Trilogía Ciencia Tecnología Sociedad https://www.redalyc.org/journal/5343/534369208004/

Sánchez, et al (2020). Los métodos de investigación para la elaboración de las tesis de maestría en educación. Pontifica Universidad Católica del Perú.

http://blog.pucp.edu.pe/blog/maestriaeducacion/2020/07/23/los-metodos-de-investigacion-para-la-elaboracion-de-las-tesis-de-maestria-en-educacion/

Sánchez, F. (2019) Fundamentos epistémicos de la investigación cualitativa y cuantitativa: consensos y disensos. *Revista Digital de Investigación en Docencia Universitaria*, 13(1), 102-122. doi: https://doi.org/10.19083/ridu.2019.644

Santacruz, H., & Hermoza, M. (2019). Los delitos informáticos y su tipificación en la legislación penal ecuatoriana. *Revista Ibérica De Sistemas e Tecnologias De Informação*, 391-400. https://www.proquest.com/scholarly-journals/los-delitos-informáticos-y-su-tipificación-en-la/docview/2318538897/se-2

Tapia, L. (2022). Tecnología y Derecho una mirada al Comercio Electrónico, el Cibercrimen y el Soft Law. *AIS: Ars Iuris Salmanticensis*, 10(1), 199–226. https://doi.org/10.14201/AIS2022101199226

Travez, N. (2018). La vulneración de los Derechos Constitucionales por la falta de tipificación de las nuevas conductas delictivas a través de las Tecnologías de Informática y Comunicación (TICs). (Trabajo de Titulación modalidad Proyecto de Investigación previo a la obtención del Título de Abogada de los Tribunales y Juzgados de la República). Universidad Central de Ecuador. http://www.dspace.uce.edu.ec/handle/25000/18733

Urpeque, C. (2019) Análisis de la adecuación de la Ley N°30096, al marco del convenio internacional de Budapest 2001, y su incidencia en la reducción de los delitos informáticos. Huaura 2018. (Tesis para optar el título de Abogado). Universidad Nacional José Faustino Sánchez Carrión. http://repositorio.unjfsc.edu.pe/handle/20.500.14067/4632

Utreras, P. (2017). LA NECESIDAD DE TIPIFICAR EL DELITO DE FRAUDE INFORMATICO EN CHILE (Memoria de prueba para optar el grado de Licenciado en Ciencias Jurídicas y Sociales). https://repositorio.uchile.cl/bitstream/handle/2250/151758/La-necesidad-

de-tipificar-el-delito-de-fraude-informático-en-Chile-análisis-jurisprudencial-doctrinario-y-normativo.pdf?sequence=1&isAllowed=y

Ventura, M. (2021) “LA TIPIFICACIÓN DEL PHISHING, SMISHING Y VISHING EN NUESTRO SISTEMA PENAL PERUANO, PARA LA LUCHA CONTRA LA CIBERDELINCUENCIA EN LIMA, 2020”. (Tesis para optar el título de abogada). Universidad Privada del Norte. https://hdl.handle.net/11537/28942

Vilca, G. (2018) LOS HACKERS: “DELITO INFORMATICO FRENTE AL CODIGO PENAL PERUANO” (Tesis para optar el título profesional de abogado). Universidad Nacional Santiago Antúnez de Mayolo http://repositorio.unasam.edu.pe/handle/UNASAM/2496

Villón, H., Sojos, M., Mendoza, C., Guarda, T., & Clery, A. (2019). Pharming y Phishing: Delitos Informáticos Penalizados por la Legislación Ecuatoriana. Revista Ibérica De Sistemas e Tecnologias De Informação, , 671-677. https://www.proquest.com/scholarly-journals/pharming-y-phishing-delitos-informáticos/docview/2195127299/se-2

Vinelli, R. (2021). DELITOS INFORMÁTICOS Y SU RELACIÓN CON LA CRIMINALIDAD ECONÓMICA. *Ius et Praxis*, (53), 95-110. https://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/4995

Vitteri, G. (2022). Mecanismos jurídicos para implementar la Ley 30096 en los Delitos Informáticos contra el patrimonio frente a las nuevas Tecnologías Informáticas. (Tesis para optar el título de Abogado). Universidad Inca Garcilaso de la Vega. http://repositorio.uigv.edu.pe/handle/20.500.11818/6461

Zerón, A. (2019). Beneficencia y no maleficencia, *Revista ADM.* 76(6), 306-307. www.medigraphic.com/pdfs/adm/od-2019/od196a.pdf

Zorrilla, K. (2018) INCONSISTENCIAS Y AMBIGÜEDADES EN LA LEY DE DELITOS INFORMÁTICOS LEY Nº 30096 Y SU MODIFICATORIA LEY Nº 30171, QUE IMPOSIBILITAN SU EFICAZ CUMPLIMIENTO. (Para optar el Título profesional de Abogado). Universidad Nacional de Ancash. http://repositorio.unasam.edu.pe/handle/UNASAM/2332

ANEXOS

Anexo A

Tabla de categorización

Problema G.	Objetivos	Categorías	Metodología	Participantes
¿cuáles son los criterios que se deben de considerar para tipificar la modalidad del *smishing* y *phishing* en la Ley de delitos informáticos? **Problema específico 1** ¿Cuáles son las razones para tipificar la modalidad del *smishing* y *phishing* en la Ley de delitos informáticos? **Problema específico 2** Cuales son las conductas delictivas del *smishing* y *phishing* en nuestra jurisdicción peruana	**O. General** Determinar los criterios que se deben de considerar para tipificar la modalidad del *smishing* y *phishing* en la Ley de delitos informáticos. **O. Específico 1** Indicar los beneficios de tipificar la modalidad del *smishing* y *phishing* en la Ley de delitos informáticos. **O. Especifico 2** Analizar las conductas delictivas del *smishing* y *phishing* en nuestra jurisdicción peruana.	Ley de delitos informáticos Ley n.° 30096 La tipificación de las conductas delictivas del s*mishing* y p*hishing*	**Tipo de investigación:** Básico **Enfoque:** Cualitativa **Diseño:** Fenomenológico **Técnica:** Entrevista y revisión documental. **Método de análisis de datos:** Hermenéutico.	Profesionales especializados en el derecho penal y procesal penal, como fiscales y abogados **Muestra:** Se contará con 2 abogados y 4 fiscales especializados en la materia de derecho penal con experiencia de más de 5 años en la provincia de Lima.

Anexo B

Instrumento de recolección de datos

GUÍA DE ENTREVISTA

Titulo:

"Inseguridad en el delito informático a través de la modalidad del *smishing* y *phishing*

INDICACIONES: El presente instrumento tiene como propósito recaudar su opinión respecto a la falta de una buena tipificación de las nuevas modalidades de delitos informáticos que es el smishing y phishing; motivo por el cual, se le pide responder las siguientes preguntas con la mayor seriedad y compromiso.

Entrevistado/a :

Cargo :

Institución :

OBJETIVO GENERAL:

Determinar los criterios que se deben de considerar para tipificar la modalidad del *smishing* y *phishing* en la Ley de delitos informáticos

Preguntas:

1. En su opinión, ¿Cuáles son los vacíos legales informáticos a consecuencia de las nuevas modalidades del *smishing* y *phishing*?

2. ¿Considera usted qué identificando los criterios que tipifiquen la modalidad del *smishing* y *phishing* sería un disuasivo para que los delincuentes no empleen esta modalidad?

3. ¿Considera usted que la tipificación del *smishing* y *phishing* reduciría considerablemente el índice de los delitos informáticos contra el patrimonio?

OBJETIVO ESPECÍFICO 1:

Indicar los beneficios de tipificar la modalidad del *smishing* y *phishing* en la Ley de delitos informáticos.

Preguntas:

4. En su opinión, ¿Considera usted que tipificando la modalidad del *smishing* y *phishing* garantizaría la seguridad jurídica?

5. En su opinión, ¿cree usted que tipificando la modalidad del *smishing* y *phishing* habría menos carpetas fiscales archivadas por la falta de una buena tipificación?

6. ¿Considera usted que tipificando la modalidad delictiva del *phishing* y *smishing* ayudaría a proteger futuros delitos subyacentes?

OBJETIVO ESPECÍFICO 2:

Analizar las conductas delictivas del *smishing* y *phishing* en nuestra jurisdicción peruana.

Preguntas:

7. En su opinión. ¿Considera que las personas que comente estos actos delictivos mediante la tecnología, son profesionales en la Tecnologías de la Información y las Comunicaciones (TIC)?

8. ¿Cree usted que el accionar de los delincuentes que cometen estos delitos están relacionados con una organización criminal?

9. En su opinión. ¿Considera que este acto de delinquir lo pueden realizar fuera de la jurisdicción peruana, para así evitar su identidad y así permanecer en el anonimato?

SELLO	FIRMA

Anexo C

Matriz de evaluación por juicio de expertos

UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado doctor en derecho: Usted ha sido seleccionado para evaluar el instrumento "Inseguridad en el delito informático a través de la modalidad del Smishing y Phishing" La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer jurídico. Agradecemos su valiosa colaboración.

1. **Datos generales del experto**

Nombre del experto:	David Arcela Collazos	
Grado profesional:	Maestría (X)	Doctor ( )
Área de formación académica:	Clínica ( ) Educativa ( )	Jurídica (X) Organizacional ( )
Áreas de experiencia profesional:	Docente	
Institución donde labora:	UCV	
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)	
Experiencia en Investigación Psicométrica: (si corresponde)	No	

2. **Propósito de la evaluación:**

Validar el contenido del instrumento, por juicio de expertos.

3. **Datos de la guía de entrevista:**

Nombre de la Prueba:	Guía de entrevista
Autor:	Diego Saul Taipe Huaman
Procedencia:	Lima Este
Administración:	El propio investigador
Tiempo de aplicación:	45 minutos
Ámbito de aplicación:	Virtual
Significación:	Se evaluó la pertinencia de las preguntas conforme a las categorías y subcategorías para generar un aporte al campo del Derecho.

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

4. Soporte teórico:

Las bases teóricas fueron de base para la elaboración de las interrogantes en la guía de entrevista.

Categoría	Subcategorías	Definición de la categoría
La ley del delito informático	La tipificación de smishing y phishing en el marco de la lucha contra el delito informático.	La incorporación en nuestro sistema jurídico peruano en la tipificación de las nuevas modalidades del delito informático que son el Smishing y Phishing

5. Presentación de instrucciones para el experto:

A continuación, a usted le presento la guía de entrevista elaborado por Diego Saul Taipe Huaman, en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

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

1. No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel (**CUMPLE**)

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

Objetivos de la investigación:

Objetivo general: Determinar los criterios que se deben de considerar para tipificar la modalidad del *smishing* y *phishing* en la ley de delitos informáticos

N.°	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
1	En su opinión, ¿Cuáles son los vacíos legales informáticos a consecuencia de la nueva modalidad del *smishing* y *phishing*?	4	3	4	
2	¿Considera usted que identificando los criterios que tipifiquen la modalidad del *smishing* y *phishing* sería un disuasivo para que los delincuentes no empleen esta modalidad?	4	4	4	
3	¿Considera usted que la tipificación del *smishing* y *phishing* reduciría considerablemente el índice de los delitos informáticos contra el patrimonio?	4	4	3	

Objetivo específico 1: Indicar los beneficios de tipificar la modalidad del *smishing* y *phishing* en la ley de delitos informático.

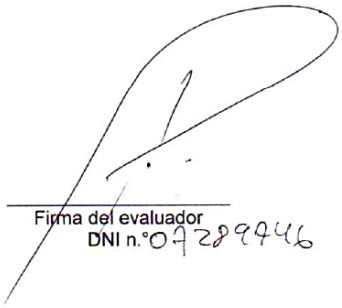
N.°	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
4	En su opinión, ¿Considera usted que tipificando la modalidad del *smishing* y *phishing* garantizaría la seguridad jurídica?	3	4	4	Ninguna
5	En su opinión, ¿Cree usted que tipificando la modalidad del *smishing* y *phishing* habría menos carpetas fiscales archivadas por la falta de una buena tipificación?	4	4	4	
6	¿Considera usted que tipificando la modalidad delictiva del *phishing* y *smishing* ayudaría a proteger futuros delitos subyacentes?	4	3	4	

Objetivo específico 2: Analizar las conductas delictivas del *smishing* y *phishing* en nuestra jurisdicción peruana.

N.°	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
7	¿Considera que las personas que comenten estos actos delictivos mediante la tecnología, son profesionales en la tecnología de la información y las comunicaciones (TIC)?	4	4	4	
8	¿Cree usted que el accionar de los delincuentes que cometen estos ilícitos están relacionados con una organización criminal?	3	4	4	
9	En su opinión, ¿Considera que este acto de delinquir lo pueden realizar fuera de la jurisdicción peruana, para así evitar su identidad y así permanecer en el anonimato?	4	4	3	

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO



Firma del evaluador
DNI n.° 07289946

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

Evaluación por juicio de expertos

Respetado doctor en derecho: Usted ha sido seleccionado para evaluar el instrumento "Inseguridad en el delito informático a través de la modalidad del *Smishing* y *Phishing*" La evaluación del instrumento es de gran relevancia para lograr que sea válido y que los resultados obtenidos a partir de éste sean utilizados eficientemente; aportando al quehacer jurídico. Agradecemos su valiosa colaboración.

1. Datos generales del experto

Nombre del experto:	Malocho Vega Luis E.	
Grado profesional:	Maestría (X)	Doctor ( )
Área de formación académica:	Clínica ( ) Educativa ( )	Jurídica (X) Organizacional ( )
Áreas de experiencia profesional:	Docente	
Institución donde labora:	UCV - UTP	
Tiempo de experiencia profesional en el área:	2 a 4 años ( ) Más de 5 años (X)	
Experiencia en Investigación Psicométrica: (si corresponde)	No	

2. Propósito de la evaluación:

Validar el contenido del instrumento, por juicio de expertos.

3. Datos de la guía de entrevista:

Nombre de la Prueba:	Guía de entrevista
Autor:	Diego Saul Taipe Huaman
Procedencia:	Lima Este
Administración:	El propio investigador
Tiempo de aplicación:	45 minutos
Ámbito de aplicación:	Virtual
Significación:	Se evaluó la pertinencia de las preguntas conforme a las categorías y subcategorías para generar un aporte al campo del Derecho.

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

4. Soporte teórico:

Las bases teóricas fueron de base para la elaboración de las interrogantes en la guía de entrevista.

Categoría	Subcategorías	Definición de la categoría
La ley del delito informático	La tipificación de smishing y phishing en el marco de la lucha contra el delito informático.	La incorporación en nuestro sistema jurídico peruano en la tipificación de las nuevas modalidades del delito informático que son el Smishing y Phishing

5. Presentación de instrucciones para el experto:

A continuación, a usted le presento la guía de entrevista elaborado por Diego Saul Taipe Huaman, en el año 2023. De acuerdo con los siguientes indicadores califique cada uno de los ítems según corresponda.

Categoría	Calificación	Indicador
CLARIDAD El ítem se comprende fácilmente, es decir, su sintáctica y semántica son adecuadas.	1. No cumple con el criterio	El ítem no es claro.
	2. Bajo Nivel	El ítem requiere bastantes modificaciones o una modificación muy grande en el uso de las palabras de acuerdo con su significado o por la ordenación de estas.
	3. Moderado nivel	Se requiere una modificación muy específica de algunos de los términos del ítem.
	4. Alto nivel	El ítem es claro, tiene semántica y sintaxis adecuada.
COHERENCIA El ítem tiene relación lógica con la dimensión o indicador que está midiendo.	1. totalmente en desacuerdo (no cumple con el criterio)	El ítem no tiene relación lógica con la dimensión.
	2. Desacuerdo (bajo nivel de acuerdo)	El ítem tiene una relación tangencial /lejana con la dimensión.
	3. Acuerdo (moderado nivel)	El ítem tiene una relación moderada con la dimensión que se está midiendo.
	4. Totalmente de Acuerdo (alto nivel)	El ítem se encuentra está relacionado con la dimensión que está midiendo.
RELEVANCIA El ítem es esencial o importante, es decir debe ser incluido.	1. No cumple con el criterio	El ítem puede ser eliminado sin que se vea afectada la medición de la dimensión.
	2. Bajo Nivel	El ítem tiene alguna relevancia, pero otro ítem puede estar incluyendo lo que mide éste.
	3. Moderado nivel	El ítem es relativamente importante.
	4. Alto nivel	El ítem es muy relevante y debe ser incluido.

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

1. No cumple con el criterio
2. Bajo Nivel
3. Moderado nivel
4. Alto nivel (**CUMPLE**)

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

Objetivos de la investigación:

Objetivo general: Determinar los criterios que se deben de considerar para tipificar la modalidad del *smishing* y *phishing* en la ley de delitos informáticos

N.°	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
1	En su opinión, ¿Cuáles son los vacíos legales informáticos a consecuencia de la nueva modalidad del *smishing* y *phishing*?	4	3	4	
2	¿Considera usted que identificando los criterios que tipifiquen la modalidad del *smishing* y *phishing* sería un disuasivo para que los delincuentes no empleen esta modalidad?	4	4	4	
3	¿Considera usted que la tipificación del *smishing* y *phishing* reduciría considerablemente el índice de los delitos informáticos contra el patrimonio?	4	4	4	

Objetivo específico 1: Indicar los beneficios de tipificar la modalidad del *smishing* y *phishing* en la ley de delitos informático.

N.°	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
4	En su opinión, ¿Considera usted que tipificando la modalidad del *smishing* y *phishing* garantizaría la seguridad jurídica?	4	4	4	Ninguna
5	En su opinión, ¿Cree usted que tipificando la modalidad del *smishing* y *phishing* habría menos carpetas fiscales archivadas por la falta de una buena tipificación?	3	4	4	
6	¿Considera usted que tipificando la modalidad delictiva del *phishing* y *smishing* ayudaría a proteger futuros delitos subyacentes?	4	3	4	

Objetivo específico 2: Analizar las conductas delictivas del *smishing* y *phishing* en nuestra jurisdicción peruana.

N.°	Ítem	Claridad	Coherencia	Relevancia	Observaciones/ Recomendaciones
7	¿Considera que las personas que comenten estos actos delictivos mediante la tecnología, son profesionales en la tecnología de la información y las comunicaciones (TIC)?	4	4	4	
8	¿Cree usted que el accionar de los delincuentes que cometen estos ilícitos están relacionados con una organización criminal?	4	4	4	
9	En su opinión, ¿Considera que este acto de delinquir lo pueden realizar fuera de la jurisdicción peruana, para así evitar su identidad y así permanecer en el anonimato?	4	4	3	

INVESTIGA UCV

UNIVERSIDAD CÉSAR VALLEJO

Firma del evaluador
DNI n.° 43448918.

INVESTIGA UCV