UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

“La regulación de las nuevas modalidades del delito informátivo en la ley N° 30096 y su modificatoria, periodo 2020-2021”

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogado

AUTORES:

Ramos Caldua, Mirian Caty (orcid.org/0000-0002-1570-6693)

Salvador Rojas, Yorman Andrey (orcid.org/0000-0003-2636-3654)

ASESORA:

Dra. Ortega Obregon, Doris Luz (orcid.org/0000-0002-3264-2011)

LÍNEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo económico, empleo y emprendimiento

HUARAZ - PERÚ

2022

Dedicatoria

Dedicamos el presente trabajo a Dios por estar con nosotros en todo momento y permitirnos cada día de vida; asimismo, a nuestros padres quienes nos acompañan en la trayectoria de nuestras vidas, brindándonos su apoyo incondicional y fortaleza.

Agradecimiento

Agradecemos a Dios y a nuestros padres, por darnos la vida, la bendición, la fuerza, el ánimo y la convicción, para obtener el resultado que anhelamos. De igual forma, a los docentes quienes ejemplarmente nos impartieron sus conocimientos, siendo un modelo académico.

Índice de contenidos

Índice de tablas

RESUMEN

La presente investigación se titula “La regulación de las nuevas modalidades del delito informático en la Ley Nro. 30096 y su modificatoria Ley Nro. 30171 en el periodo 2020-2021”, tiene como objetivo fundamentar la regulación de las nuevas modalidades del delito informático en la Ley Nro. 30096 y su modificatoria Ley Nro. 30171. Asimismo, la investigación realizada fue de enfoque cualitativo, tipo aplicada, nivel descriptivo y diseño de teoría fundamentada; donde el escenario de estudio fue el ordenamiento jurídico peruano siendo esta la Ley Nro. 30096, Ley de Delitos Informática y su modificatoria Ley Nro. 30171, con la participación de 5 fiscales de las Fiscalías Provinciales Penales Corporativas de la ciudad de Huaraz. Obteniendo como resultado que la falta de una regulación específica de las nuevas modalidades del delito informático, generan el incremento de este tipo de conductas delictivas e impunidad. Concluyendo que las nuevas modalidades del delito informático (Phishing, Smishing y Vishing), deben ser incorporadas dentro de la Ley de Delitos Informáticos a fin de ser sancionadas.

Palabras Clave: Delito Informático, Phishing, Smishing y Vishing.

ABSTRACT

The present investigation is entitled "The regulation of the new modalities of computer crime in Law No. 30096 and its amendment Law No. 30171 in the period 2020-2021", aims to base the regulation of the new modalities of computer crime in Law No. 30096 and its amending Law No. 30171. Likewise, the research carried out had a qualitative approach, applied type, descriptive level and grounded theory design; where the study scenario was the Peruvian legal system, this being Law No. 30096, Law on Computer Crimes and its amendment Law No. 30171, with the participation of 5 prosecutors from the Corporate Criminal Provincial Prosecutors of the city of Huaraz. Obtaining as a result that the lack of a specific regulation of the new modalities of computer crime, generate the increase of this type of criminal behavior and impunity. Concluding that the new modalities of computer crime (Phishing, Smishing and Vishing), must be incorporated into the Computer Crime Law in order to be sanctioned.

Keywords: Computer Crime, Phishing, Smishing and Vishing.

I. INTRODUCCIÓN

A partir del año 2020 ante el incremento de contagio del Covid-19, los gobiernos tomaron la radical decisión del confinamiento domiciliario; por ende, las actividades que se realizaban de manera presencial tuvieron que adaptarse a la modalidad virtual, ello incluye, las clases educativas, comercio, trabajo, eventos sociales, entre otros; llegando a ser, clases virtuales, e-comerse, trabajo remoto, eventos zoom, lo cual implico una "nueva realidad" para las personas al tener que adaptarse a realizar sus actividades desde su hogar, de manera que el tránsito de dinero en efectivo se convirtió a pago por medios digitales (bancas móviles o plataformas de pago, monederos virtuales), provocando un incremento en el uso de la tecnología.

Por ende, si bien es cierto la evolución de la tecnología a lo largo del tiempo sin lugar a dudas ha beneficiado a muchos de los ciudadanos en sus quehaceres del día a día y desarrollo del mismo; sin embargo, también ha beneficiado a los ciberdelincuentes en la comisión de ilícitos penales originando nuevas formas de cometer delitos. En consecuencia, tanto el uso de la tecnología como el avance del mismo ha generado en el país el surgimiento de nuevas modalidades de delitos informáticos, que al convertirse en delitos más sofisticados dificultan su persecución.

También debemos denotar que nuestro ordenamiento jurídico regula los delitos informáticos los cuales se encuentran centrados en sancionar conductas antijurídicas cometidas mediante los medios digitales por vulneraciones de seguridad cibernética, clonación de información e interferencias en sistemas informáticos; empero, no se regula de forma precisa las nuevas modalidades de delito informático como son el Phishing, el Smishing y el Vishing; conductas que incrementaron a la par del desarrollo de nuevas tecnologías y soportes tecnológicos.

En ese sentido, el diario oficial "El Peruano" nos refleja el incremento de estos ciberdelitos cometidos durante enero y abril del año dos mil veintiuno, precisando que se investigaron 1.188 denuncias por fraudes informáticos, realizadas a través de redes sociales, correos masivos, mensajes de texto, y sitios webs falsos, teniendo como la modalidad más frecuente el Phishing.

De igual forma, la Oficina de Análisis Estratégico Contra la Criminalidad – OFAEC del Ministerio Público - MP (2021), refiere que el incremento en la ciberdelincuencia se debe al desarrollo tecnológico informático, puesto que la tecnología es aquel medio que crea nuevas oportunidades de delinquir aumentando la tasa y diversidad de delitos, precisando que en el Perú las cifras de denuncias en el Ministerio Público por delitos informáticos incrementaron aceleradamente al pasar los años.

Asimismo, la página web del gobierno nacional peruano en octubre del 2021 refiere que ha existido un incremento de denuncias desde el 2013 hasta el 2021 registrando un total de 21,687 denuncias, cabe resaltar que ante tal incremento el gobierno peruano a través del Ministerio Público creó una Unidad Especializada en Ciberdelitos o Ciberdelincuencia, la misma que utilizará nuevos medios tecnológicos como soportes para poder recabar pruebas. Sin embargo, estas pruebas tomarían menos relevancia al no poder enmarcarse correctamente dentro de la Ley de Delitos Informáticos.

Por ende, como problema general se planteó la siguiente pregunta:

¿De qué manera la Ley Nro. 30096 y su modificatoria Ley Nro. 30171 regularían las nuevas modalidades del delito informático en el periodo 2020-2021?

Como problemas específicos se planteó las siguientes interrogantes:

PE1: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Phishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?

PE2: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Smishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?

PE3: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Vishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?

La investigación, tiene por justificación la necesidad de poder incorporar las nuevas modalidades del delito informático dentro de la Ley de Delitos Informáticos; asimismo, tiene el objetivo de proporcionar un alcance acerca de las conductas delictivas de Phishing, Smishing y Vishing las cuales no se encuentran definidas

claramente por el ordenamiento jurídico; sin embargo, los casos dados bajo esta modalidad han ido en incremento, es por ello, que existe una necesidad de poder investigar los sujetos, las modalidades y los medios empleados para la ejecución de estos delitos, tratando de dar una luz referente a su tipificación. Consecuentemente, se parte de la necesidad normativa, puesto que a pesar de existir una Ley que regula y establecen los delitos informáticos, la incorporación de las nuevas modalidades vendría a ser un aporte en el plano jurisdiccional, ya que la sanción por la comisión de estos delitos aún se encuentra en desarrollo.

Se planteó, los siguientes objetivos:

OG: Fundamentar la regulación de las nuevas modalidades del delito informático en la Ley Nro. 30096 y su modificatoria Ley Nro. 30171 en el periodo 2020-2021.

OE1: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Phishing como nueva modalidad del delito informático, en la Ley N° 30096 y su modificatoria Ley N° 30171, en el periodo 2020-2021

OE2: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Smishing como nueva modalidad del delito informático, en la Ley N° 30096 y su modificatoria Ley N° 30171, en el periodo 2020-2021

OE3: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Vishing como nueva modalidad del delito informático, en la Ley N° 30096 y su modificatoria Ley N° 30171, en el periodo 2020-2021

II. MARCO TEÓRICO

Al respecto, se tiene como **antecedentes internacionales** a:

En Argentina, Salvi (2019) en su tesis titulada: “El Phishing en la Argentina”, con el objetivo de analizar el problema del “Phishing” como medio de comisión del delito informático y su conexión con la legislación argentina, además analizar la Ley N° 26.388 y los vacíos normativos. Aplicando la investigación cualitativa, con escenario de estudio la Ley N° 26.388. Concluyendo que la Ley de Delitos Informáticos requiere ser modificada y actualizada, a fin de evitar los vacíos normativos. Respecto al Phishing se debe establecer tratados o acuerdos que permitan una colaboración mutua entre países para erradicar la criminalidad informática.

En Colombia, Ribero (2016) en su investigación: Delitos Informáticos y su legislación en el contexto Colombiano. Retos Sociales y Tecnológicos Nacionales. Con el objetivo de estudiar los delitos informáticos y su legislación colombiana desde el ámbito social y el ámbito tecnológico. Tipo de investigación cualitativa, aplicando las técnicas de entrevistas, revisión de documentos, registro de historia, etc. Concluyendo que el delito informático ocasiono millonarias pérdidas debido a que es considerado como uno amenaza del siglo XXI, ya que mientras la tecnología avance las maneras de cometer delitos son más, en consecuencia, dichas normas deben avanzar en la misma medida. De allí que, en Colombia la mayor cantidad de denuncias por robos informáticos son en la modalidad de Phishing.

En Bolivia, Montaño (2019) en su tesis "La tipificación penal del Phishing, como medida de seguridad informática para contener delitos informáticos", que tuvo como objetivo establecer la necesidad de incorporar el Phishing en el Código Penal como delito informático a fin de garantizar el derecho a la propiedad y evitar la impunidad. La investigación utilizo el método jurídico, deductivo, inductivo y analítico comparativo, utilizando la técnica de revisión documental y entrevista. Concluyendo que el Phishing se vincula con el delito de Estafa, ya que el objetivo que persigue es el beneficio económico; empero, se diferencia por el medio utilizado (tecnología), razón esencial para incorporarlo como tipo penal independiente debido a su incremento en gran magnitud, además de no encontrarse tipificada como delito.

Asimismo, se abordaron como **antecedentes nacionales**:

En Chiclayo, Fuentes (2021) en su tesis titulada: Modificación de la Ley N° 30096 para incorporar los delitos de Phishing, Pharming y Carding como delitos penalizables con prisión, para reducir la ciberdelincuencia, Lima 2019; cuyo objetivo es justificar la incorporación de dichos delitos en la Ley Nro. 30096, con una sanción de pena privativa. La investigación es cualitativa, tipo básica, de diseño no experimental. Escenario de estudio la Ley N° 30096, con participación de normas jurídicas sobre delitos informáticos. Utilizando el instrumento de ficha de análisis documental. Concluyendo, que la Ley N° 30096 regula el medio por el que se comete el ilícito informático más no la conducta específica; asimismo, indica que la norma es deficiente en cuanto a la tipificación del Phishing, Pharming y Carding.

En Huaraz, el autor Vilca (2018) en su investigación “Los Hackers: Delito Informático frente al Código Penal Peruano”. Tuvo como objetivo conocer la laguna normativa del Código Penal respecto a las comunicaciones electrónicas comerciales. Tipo de investigación jurídico descriptiva, dogmática de enfoque cualitativo, de diseño de investigación no experimental. Escenario de estudio es el Código Penal del Perú, la Ley N° 30096 y su modificatoria. Empleando el instrumento de análisis documental, fichas ya sean textuales, comentario, resumen, critica y cuestionario de encuesta. Finalmente, concluye que el Perú regula los delitos informáticos de forma deficiente y general, propiciando vacíos normativos que dificultan en gran medida una investigación en materia informática.

En Chimbote, los autores Hildalgo y Solano (2021), en su tesis “El Phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano, propuesta de incorporación del artículo 7-a en la Ley de Delitos Informáticos 30096”, cuyo objetivo fue desarrollar aquellos fundamentos para regular el Phishing en la normatividad peruana y evitar la impunidad. Mediante una investigación de enfoque cualitativo, aplicada, de nivel descriptivo y de diseño de teoría fundamentada. Unidad de análisis o participantes los fiscales penales del Santa, utilizando la técnica de fichaje y encuesta, bajo el instrumento de fichas bibliográficas, de resumen, textuales y cuestionario. Concluyendo que, los tipos penales del Código y la Ley no subsumen ni permiten subsumir el Phishing, ocasionando de esa manera la impunidad. Por lo que, es necesario crear tipo penal específico.

Por lo que, para tener un mejor entendimiento respecto a los delitos cometidos por medios tecnológicos, se ha de partir definiendo el **delito informático** como aquella actividad que por medio del uso de computadoras se comete cierto delito incluyendo nuevas modalidades y empleo de elementos como es el internet (Sánchez et al, 2018, p. 180).

Es decir, el delito informático es aquella conducta delictiva por medio de la utilización de un elemento informático como es el internet, la misma que supone un sin fin de modalidades delictivas.

Por su parte, Acosta et al (2020) precisa que el delito informático es aquel comportamiento o conducta ilícita cometida por medio del uso inadecuado de la tecnología, de manera que dicho comportamiento atenta contra la privacidad que

tiene el usuario respecto a su información, ya que se extraen sus datos personales (p. 351); por lo que, dichos comportamientos ilícitos suceden en el ciberespacio.

Asimismo, doctrinariamente el delito informático se ha caracterizado por englobar las palabras del ciberdelito, el cibercrimen o la ciberdelincuencia, debido a que como alude el autor Pons (2017) este tipo de delitos describen aspectos ilícitos cometidos en el espacio cibernético y se caracterizan por ser cometidos sin dificultad alguna, con la utilización de pocos recursos, en cualquier jurisdicción y por la falta de tipificación y sanción (p. 87).

Dicho de otra manera, si bien es cierto en el Perú algunos de estos delitos se encuentran regulados y sancionados; sin embargo, se da la existencia de nuevas modalidades que no se encuentran previstas como tal, lo cual implica una mayor abundancia en la realización de estos delitos.

Es así, que en la legislación peruana en el año 2000 se incorporaron por primera vez al Código Penal los Delitos Informáticos mediante la Ley Nro. 27309, los mismos que se encontraban establecidos en el Libro Segundo, correspondiente a la Parte Especial, dentro del Título V referente a los Delitos Contra el Patrimonio, en específico en el Capítulo X sobre Delitos Informáticos; posteriormente, en el año 2013, se promulgó y público la Ley de los Delitos informáticos, Ley Nro. 30096, a fin de sancionar aquellas conductas ilícitas que utilizan la tecnología en aras de proteger el bien jurídico de este tipo de delitos como es la información, los datos informáticos, la confiabilidad, la integridad, etc. Y finalmente, en el año 2014 se publicó la Ley Nº 30171, Ley destinada a modificar la Ley de Delitos Informáticos.

En ese sentido, actualmente la norma encargada de regular todos aquellos delitos informáticos (Ley Nro. 30096) y su modificatoria, tienen como objetivo primordial la prevención y sanción de las conductas o comportamientos ilícitos que se cometen a través del uso de la tecnología y afecta el bien jurídico de una persona; de manera que, pretende garantizar y proteger los derechos, así como luchar contra los ciberdelitos (Art. I. Ley Nro. 30096).

Empero, sin duda alguna, dichas normas de seguridad se han ido deteriorado en el contexto de confinamiento a raíz del COVID-19, por no encontrarse preparados para el trabajo remoto; razón por la cual, el número de víctimas de los delitos informáticos solo van en incremento en el tiempo (Bokovnya et al, 2020, p. 471).

Por ende, la legislación peruana si bien regula diversa modalidades del delito informático; sin embargo, dicha figura jurídica al ser un delito cometido a través del uso tecnológico se convierte en un medio idóneo para la generación de **nuevas modalidades delictivas** como son las estafas, robos o fraudes informáticos, o las conductas delictivas del Phishing, Smishing, Vishing, etc.

Para, los autores Altwairqi et al (2019) las variantes de los ataques dependen del desarrollo de la tecnología, ya que las mismas también desarrollan nuevos métodos para obtener diversas oportunidades para crear un ataque, de manera que estos ataques se ramifican en varios tipos como son el Phishing, Smishing y Vishing.

De la misma manera, el autor Devia (2017) manifiesta diversas modalidades de estafa informática mayormente utilizadas, entre las cuales encontramos al Phishing mediante el uso del correo electrónico; el Smishing, a través de mensajes o SMS; y finalmente, encontramos al Vishing dada a través de llamadas telefónicas. Igualmente, Banire et al (2021) manifiesta que identificaron al Phishing, Smishing y Vishing como los ataques más comunes y oscuros para los usuarios (p. 01).

Por consiguiente, para mayor abundancia a continuación se precisarán algunas de las nuevas modalidades del delito informático:

El Phishing, para Diaz y Hernández (2021) es aquella conducta ilícita que utiliza el correo electrónico a través de los emails para redireccionar a los usuarios a páginas falsas donde se solicitan datos confidenciales (p. 19). En otras palabras, el Phishing es la obtención de datos personales del usuario de manera fraudulenta mediante el favorecimiento de la tecnología (Mayer y Oliver, 2020).

De ahí que, es considerado como aquel sistema de pesca de datos confidenciales, a través de plataformas engañosas que simulan ser una página oficial, por ejemplo, las plataformas virtuales bancarias donde simulan ser el banco para poder apoderarse de la información personal a fin de obtener un beneficio económico.

Por tanto, en esta nueva modalidad de delito informático existen dos clases de sujetos, como alude Parada y Errecaborde (2018) por un lado encontramos a los phishers, estafadores o sujeto activo y por otro lado encontramos a los cibernavegantes, usuarios o sujeto pasivo (p. 40).

La figura o conducta dada en el Phishing se configura por medio del uso de correos electrónicos a modo de anzuelo, a fin de pescar a las víctimas mediante el engaño para que proporcionen su información personal (Villón et al, 2019, p. 673).

Dicho de otro modo, se configura con la captación de manera ilícita de los datos mediante el link o URL enviado al correo electrónico, el mismo que solicita al receptor una gran diversidad de información personal como son los datos personales, número de tarjetas, claves, etc., todo ello mediante el engaño.

Por su parte, García (2018) señala que la conducta del Phishing es enviar emails fraudulentos desde una dirección supuesta de una entidad al correo electrónico del usuario, solicitando datos personales como cuentas y contraseñas a fin de obtener un beneficio económico. Es decir, enviar emails con contenido malicioso a fin de robar las contraseñas y otros datos para obtener cierto provecho (Esparta, 2022).

En consecuencia, el bien jurídico protegido en esta modalidad al igual que los demás en sentido común es el patrimonio; empero, como señalan los autores Hidalgo y Solano (2021) protege en sentido estricto la confidencialidad de la información (sensible); es decir, la información personal del usuario.

Al respecto, el **Smishing** es aquel ciberataque mediante el cual se envía un SMS o mensaje de texto, que suplanta la comunicación oficial y engaña a los usuarios para robarles sus datos personales y demás informaciones (García, 2020, p. 6).

Es decir, mediante la suplantación de identidad se envía un mensaje al celular, con el único propósito de conseguir información confidencial de la víctima y de esa manera beneficiar al delincuente para cometer estafas de manera electrónica.

Es así, que el autor Paiva (2021) refiere que en este tipo de modalidad se usa un canal de comunicación distinto, el cual es por medio del envío de SMS al celular del usuario suplantando la identidad generando confianza, con la sola intención de adquirir mayores datos del usuario para obtener cierto provecho (p. 30).

De manera que, los delincuentes envían dichos mensajes o SMS por aquellas aplicaciones del teléfono celular más usadas por la sociedad como el Facebook, WhatsApp, Telegram, etc., todo ello a fin de sustraer información.

Es por ello, que en el Smishing se produce la participación del criminal o delincuente encargado de enviar el SMS a fin de obtener datos; y, la victima o usuario quien ingresa a la web o URL falso que fue enviado en el SMS (Diaz y Hernández, 2021).

Por lo que, en muchas de las ocasiones al sujeto activo se le conoce como smisher, debido a que es quien ejecuta el acto mediante el envío del SMS y al sujeto pasivo se le conoce como usuario o víctima, siendo este el receptor de dicho mensaje.

En ese sentido, la conducta dada en el Smishing, es enviar SMS o mensajes de texto maliciosos al usuario a través de los cuales se le solicita que remitan su información confidencial (Mishra y Soni, 2020). Por tanto, el bien jurídico protegido es la información personal y los datos confidenciales del usuario (Diaz y Hernández, 2021); además, se considera como bien protegido al patrimonio.

En cuanto, al **Vishing** es aquella figura delictiva que se configura mediante llamadas telefónicas engañosas a fin de entablar una comunicación con la victima valiéndose de una suplantación de identidad para recabar información confidencial (Paredes, 2021, p. 07). Y es dada a través de las telecomunicaciones como refiere la Oficina de las Naciones Unidas contra la Droga y el Delito - UNODC (2020).

Dicho de otra manera, esta modalidad emplea la voz a través de las llamadas telefónicas, indicando ser empresas legítimas y en muchas de las ocasiones inicia con la recreación de una voz automatizada para posteriormente pasar la llamada a un supuesto asesor, a fin de conseguir información financiera de la víctima.

Por otro lado, los autores Kalaharsha y Mehtre (2021), consideran al Vishing como un tipo de fraude telefónico que utiliza mensajes de voz para obtener información personal de las víctimas, solicitando números de cuentas u otros datos personales.

En ese sentido, el Vishing al igual que las modalidades anteriormente abordadas cuenta con la participación del sujeto activo conocido como visher, quien busca engañar mediante llamadas telefónicas; asimismo, el sujeto pasivo es conocido como usuario o víctima, quien es engañado para brindar sus datos personales.

Es así que, la conducta dada en el Vishing es realizar una llamada al teléfono celular de la víctima haciéndose pasar por una empresa confiable; por ejemplo, simular ser una entidad bancaria, un proveedor de seguros, entre otros; a fin de lograr obtener información confidencial del usuario (Njuguna et al, 2022, p. 10).

Por consiguiente, el bien jurídico protegido al respecto como indica Ventura (2021) es la seguridad informática; es decir, la protección de los datos y el bienestar del usuario respecto a su información confidencial.

Finalmente, respecto al derecho comparado las nuevas modalidades del delito informativo aumentaron al igual que el uso de los medios tecnológicos, por lo que se han establecido sanciones para las mismas en algunos casos:

En el país de Colombia, la Ley N° 1273 del año 2009, regulo los delitos informáticos dentro del Código Penal Colombiano (Ley N° 599 de 2000) en el Título VII BIS con la denominación “De la Protección de la información y de los datos”, dentro de los artículos del 269A al 269H, normativa que penaliza los ciberdelitos, como el Phishing y demás modalidades específicamente reguladas en el artículo 269G respecto a la suplantación de sitios web para capturar datos personales, que establece una sanción de prisión y multa al que con objeto ilícito (…) desarrolla, realiza programaciones, ejecute o realice envíos de páginas electrónicas, enlaces o ventanas emergentes (Medina et al, 2021).

En Argentina, como precisa el autor Salvi (2019) actualmente las nuevas modalidades del delito informático no están reguladas como tal; sin embargo, pueden subsumirse dentro del tipo penal de estafa regulada en el Art. 173 inciso 16 del Código Penal Argentino, incorporado mediante Ley 26.388, que sanciona aquella conducta realizada con ardid o engaño a fin de obtener datos de la víctima y realizar una transferencia bancaria, adquirir bienes o servicios a nombre de la víctima, generando un perjuicio patrimonial.

De igual forma, en el país de España, las nuevas modalidades del delito informático se subsumen dentro del delito de estafa dada mediante la manipulación informática, prescrita en el Código Penal Español específicamente en el artículo 248.2 letra a), que establece tanto el ánimo de lucro del agente como la manipulación o artificio informatice a fin de conseguir un beneficio sin consentimiento alguno (Devia, 2017).

Asimismo, en Alemania por medio de la segunda ley de lucha contra la criminalidad económica del año 1986, se incluyó al Código Penal Alemán, el delito de Estafa por computador en el artículo 263a que establece una sanción para aquel que a fin de obtener una ventaja patrimonial utiliza datos no autorizados.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

3.1.1. Tipo de investigación

Al respecto, los autores Pimienta y De la Orden (2017) refieren que el tipo de investigación aplicada es aquella que busca la consolidación de un saber y la aplicación de conocimientos culturales, científicos, etc., en servicio de la población (p. 9).

Es así que, el estudio realizado es de enfoque cualitativo, de tipo de investigación aplicada, de nivel descriptivo, ya que se realizó la fundamentación y explicación para regular las nuevas modalidades de delitos informáticos en la legislación del Perú, a fin de sancionar dichas conductas delictivas.

3.1.2. Diseño de investigación

Para Hernández et al (2017) el diseño de teoría fundamentada se caracteriza por producir una explicación de un proceso, interacción, fenómeno o acción aplicada a un entorno en concreto, desde la perspectiva de distintos participantes, ya sea de manera genérica o teórica.

Al respecto, el presente proyecto es de diseño de teoría fundamentada, debido a que se abordó la explicación del desarrollo de la investigación de las nuevas modalidades del delito informático y su incorporación a la Ley de Delitos Informáticos.

3.2. Categorías, Subcategorías y matriz de categorización

CATEGORÍAS	SUBCATEGORIAS
PHISHING	• Web • Correos electrónico • Sujetos • Conducta • Bien jurídico protegido
SMISHING	• SMS • Mensajes • Sujetos

	• Conducta • Bien jurídico protegido
VISHING	• Voz • Llamadas • Sujetos • Conducta • Bien jurídico protegido

3.3. Escenario de estudio

Dentro del ordenamiento jurídico peruano se establecen normas específicas para regular el delito informático, siendo estas las más adecuadas para prescribir las nuevas modalidades del delito informático; por lo tanto, el escenario geográfico dentro del ámbito espacial en la presente investigación es el Perú, en específico la Ley Nro. 30096 Ley de los Delitos informáticos y la Ley Nro. 30171 que modifica la misma.

3.4. Participantes

En el presente proyecto, los participantes fueron 5 fiscales del Distrito Fiscal de Áncash, correspondiente a las Fiscalías Provinciales Penales Corporativas de la ciudad de Huaraz.

3.5. Técnicas e instrumentos de recolección de datos

Los autores Pimienta & De la Orden (2017) consideran a las técnicas como procedimientos, observaciones, encuestas, entrevistas, etc.; mediante los cuales se realizan recopilaciones de datos u informaciones durante una investigación, con el apoyo de instrumentos (p. 162). Por ende, la técnica utilizada en la presente fue la entrevista.

En referencia al instrumento, es considerado como aquel medio en el que se registran interrogantes, afirmaciones u proposiciones respecto al objeto de estudio, con la finalidad de obtener datos para ser evaluados, analizados e interpretados (Tacilio, 2016, p. 70). Es así, que se empleó el instrumento de guía de entrevista el cual permitió realizar la recopilación de datos de la información.

3.6. Procedimiento

Tóala y Briones (2019) mencionan que la indagación científica es un conjunto de procedimientos los cuales permitirán la creación de un conocimiento pertinente y

de manera actualizada teniendo un rigor académico dentro de las instituciones universitarias. Por ende, se realizó el siguiente procedimiento: 1) Investigación problemática; 2) Identificación de la realidad problemática; 3) Planteamiento del problema; 4); Delimitación de la espacialidad y temporalidad; 5) Búsqueda de información documentaria; 6) Recopilación de información doctrinaria; 7) Procesamiento y análisis de la información doctrinaria; 8) Elección de participantes; 9) Elaboración y aplicación del instrumento; 10) Análisis, elaboración de resultados y discusión; 11) Conclusiones y recomendaciones.

3.7. Rigor científico

Al respecto, el autor Hernández et al (2016) señalan que una investigación o indagación cualitativa debe de caracterizarse por ser un trabajo de calidad, la misma que debe de cumplir cabalmente con el rigor científico, conocido también como validez o confiabilidad; la cual, establece una serie de criterios para su determinación y aceptación, entre los cuales encontramos: Primero, la dependencia definida como la confiabilidad o consistencia lógica que implica la revisión y verificación de los datos por investigadores; segundo, la credibilidad es conocida también como la máxima validez y definida como la captación profunda de las experiencias de los participantes; tercero, la transferencia conocida por el termino traslado referida a la transmisión de la información por medio de un trabajo científico a la realidad de la sociedad; mediante la perspectiva del investigador; cuarto, la confirmación llamado también conformabilidad termino relacionado con el criterio de credibilidad ya que permite el rastreo de datos a fin de ser interpretados; y finalmente, otros criterios complementarios como la fundamentación, aproximación, etc.

3.8. Método de análisis de datos

Referente al presente punto, el método utilizado son los siguientes: primero, el método descriptivo debido a que se describen las nuevas modalidades de los delitos informáticos en la legislación del Perú a fin de sancionar dichas conductas delictivas y ser reguladas dentro de la Ley; segundo, el método analítico, puesto que se analizó las respuestas de los participantes; tercero, el método inductivo, ya que fue empleada a fin de reunir y analizar la información doctrinaria a fin de poder obtener respuestas; así como también, poder expandir y descubrir nuevos

conocimientos respecto de las nuevas modalidades de los delitos informáticos; cuarto, el método hermenéutico, debido a que se analizó textos, para una mejor comprensión temática y quinto, el método interpretativo, puesto que permitió una mejor comprensión de la información o resultados obtenidos mediante el instrumento correspondiente.

3.9. Aspectos éticos

La presente investigación, fue dada bajo los parámetros de originalidad, cumpliendo a cabalidad con la Guía de Elaboración de Productos de Investigación de Fin de Programa, de la Universidad César Vallejo. Asimismo, se cumplió con el respeto de la propiedad intelectual debido a que se utilizó de manera adecuada tanto las citas como referencias bibliográficas cumpliendo las reglas de American Psychological Association – APA 7° (séptima edición).

IV. RESULTADOS Y DISCUSIÓN

Resultados:

El presente capitulo comprende en primer lugar los resultados obtenidos después del proceso de recolección, análisis y tratamiento de datos recabados mediante la entrevista realizada a 5 Fiscales de las Fiscalías Penales Corporativas – Distrito Fiscal de Ancash, de la ciudad de Huaraz.

Inicialmente, se realizaron preguntas genéricas respecto al ámbito temático que tuvo como **objetivo general**: Fundamentar la regulación de las nuevas modalidades del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171:

Tabla 1: *Información especializada en delitos informáticos.*

Pregunta N° 01: ¿Usted recibió charlas informativas, capacitaciones o cursos especializados en delitos informáticos, ofrecidas por el Ministerio Público u otra entidad? Precise.				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**

Nunca he recibido capacitación o curso alguno respecto a este tipo de delitos por la fiscalía, empero, mi persona asistió a capacitaciones ofrecidas por el Poder Judicial.	No, por parte de la fiscalía no he recibido capacitación; sin embargo, a merito personal me he capacitado.	No recibí capacitación sobre delitos informáticos.	Por parte del Ministerio Publico no he recibido capacitación especializada en el tema en mención, pero si me capacite asistiendo a cursos especializados.	No recibí información alguna respecto al delito informático.
Interpretación: En su totalidad los participantes mencionaron que no recibieron capacitación alguna por parte del Ministerio Publico respecto a delitos informáticos; sin embargo, tres de los participantes se capacitaron de manera personal.				

Tabla 2: *Denuncias sobre delitos informáticos.*

Pregunta N° 02: ¿Durante el periodo 2020 al 2021 las denuncias en su despacho respecto a delitos informáticos incrementaron? De ser afirmativa su respuesta precise ¿Por qué?				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**
Considero que debido al confinamiento social y el mayor uso de los medios tecnológicos se ha incrementado la comisión de estos delitos, teniendo en mi despacho un gran incremento al respecto.	Si, se incrementaron debido al uso constante de la tecnología por épocas de pandemia, por el Covid-19 ya que todo se realizó virtualmente.	Si se incrementaron, puesto que en esos años la virtualidad estuvo en auge.	En este despacho fiscal si se han incrementado los casos durante ese periodo. Considero que el motivo es por el avance de la tecnología.	Si incrementaron por que se denoto mayor ingreso de denuncias respecto a delitos informáticos.
Interpretación: La totalidad de los participantes concordaron en que los delitos informáticos durante el periodo 2020 al 2021 incrementaron en los despachos fiscales.				

Tabla 3: *Las nuevas modalidades de delito informático.*

Pregunta N° 03: ¿La falta de regulación específica de las nuevas modalidades del delito informático generan impunidad? ¿Por qué?				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**
Si generan impunidad porque el surgimiento de las nuevas modalidades del delito informático al no estar reguladas, no pueden ser tipificadas correctamente, ni sancionadas.	Si generan impunidad siempre en cuando no se puedan tipificar como otro delito.	Si generan impunidad puesto que no hay una regulación en la norma que específicamente sancione estos delitos sino solo de manera genérica.	Considero que si generan impunidad debido a que mientras más avance la tecnología a la par debería avanzar la regulación de la norma existiendo una regulación específica.	Si, ya que no hay norma específica para imputar delito alguno.
Interpretación: Los participantes indicaron que existe impunidad debido a que las nuevas modalidades del delito informático no cuentan con una regulación específica, por ende, no pueden ser sancionadas en virtud a un tipo penal.				

Tabla 4: *Regulación específica de las nuevas modalidades de delito informático.*

Pregunta N° 04: ¿Considera que las nuevas modalidades del delito informático deberían encontrarse reguladas en la Ley Nro. 30096, su modificatoria Ley N° 30171 o en el Código Penal? ¿Por qué?				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**
Si deberían regularse porque permitiría enmarcar de manera adecuada tal conducta delictiva a fin de sancionarse.	Si considero que se deberían encontrar reguladas, sobre todo en el Código Penal ya que es la norma base que permite	Considero que debería encontrarse regulado en la ley N° 30096 y su modificatoria porque nos permitiría tipificarlo de	Si, tal como mencione anteriormente las normas deben regular las nuevas conductas delictivas que surgen a raíz del avance tecnológico.	Si deberían regularse porque nos permitiría tipificar mejor estos delitos.

	sancionar los delitos.	manera específica.		
Interpretación: La totalidad de participantes coincidieron en que las nuevas modalidades del delito informático deberían regularse en una ley específica o en el Código Penal, a fin de ser sancionadas y evitar que dichas conductas delictivas queden impunes.				

Respecto al **primer objetivo específico**: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Phishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021. Se formuló las siguientes preguntas:

Tabla 5: *Casos referentes al Phishing.*

Pregunta N° 05: ¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Phishing? De ser afirmativa su respuesta, especifique la cantidad.				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**
Se me han presentado varios casos referentes al Phishing, en un total de nueve casos a lo largo de mi carrera fiscal.	Si he tenido un caso.	En mi carrera fiscal tuve un caso de Phishing.	Si tuve cuatro casos sobre este tipo de conducta delictiva.	Si se presentaron cinco casos referentes al Phishing.
Interpretación: Los participantes refirieron haber tenido un caso o más referentes a la conducta delictiva de Phishing durante el tiempo que han laborado en la fiscalía.				

Tabla 6: *Tipificación alterna al Phishing.*

Pregunta N° 06: ¿Cómo tipificó usted la conducta delictiva del Phishing?				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**
Dos casos de Phishing fueron tipificados como estafa agravada, en un caso como	Lo tipifique como delito de Estafa debido a que en nuestra norma no existe una regulación	Como estafa lo tipifique	Dichas carpetas fiscales que ingresaron a mi despacho fueron tipificadas de	Tipifique como delito de Estafa de acuerdo al artículo 196

delito contra el patrimonio de manera genérica y seis casos como el delito de estafa.	específica del Phishing		manera genérica como Delitos Contra el Patrimonio.	del Código Penal.
Interpretación: Los entrevistados respondieron que han tipificado como Estafa, Estafa Agravada y de manera genérica como delitos contra el Patrimonio.				

Tabla 7: *Estado procesal de los casos de Phishing.*

Pregunta N° 07: ¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Phishing?				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**
En etapa preliminar siete carpetas fiscales fueron archivadas y dos de ellas llegaron a formalizarse pasando a la etapa de acusación.	Esta carpeta fue archivada en etapa preliminar	El estado procesal es de archivo en preliminar.	Todas fueron archivadas en etapa preliminar, por falta de pruebas.	Una carpeta fiscal se encuentra formalizada y las otras carpetas fueron archivadas en etapa preliminar.
Interpretación: La mayoría de participantes sostuvieron que el último estado procesal de las carpetas fiscales que tuvieron a su cargo fueron archivadas en etapa preliminar.				

Tabla 8: *Incorporación específica del Phishing.*

Pregunta N° 08: ¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Phishing? ¿Por qué?				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**
Desde mi perspectiva, si se debería regular, ya que siendo así se	Si, considero como anteriormente mencione que se debe encontrar regulada en el	Si se debería incorporar, porque es la herramienta para sancionar los	Sí, porque de esa manera las conductas de Phishing serían sancionada.	Si debería incorporarse un tipo penal para que todas las carpetas fiscales

sancionaría tal conducta.	Código Penal, para que permita una formalización en los casos referentes a Phishing.	delitos informáticos.		puedan formalizarse y no se genere impunidad.
Interpretación: El total de los participantes señalaron que la conducta delictiva del Phishing debería regularse en nuestra legislación como un tipo penal específico con la finalidad de sancionar tal acción.				

En cuanto al **segundo objetivo específico:** Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Smishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021; se tiene las siguientes preguntas,

Tabla 9: *Casos referentes al Smishing.*

Pregunta N° 09: ¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Smishing? De ser afirmativa su respuesta, especifique la cantidad.				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**
Se me presentaron seis casos de Smishing.	Si he tenido cuatro casos referentes al Smishing.	En mi carrera Fiscal tuve cuatro casos de Smishing.	Si tuve seis casos dentro de mi carrera fiscal.	En mi carrera fiscal tuve cuatro carpetas fiscales referentes a esta conducta.
Interpretación: Los participantes indicaron que a lo largo de su carrera fiscal se le presentaron de cuatro casos a más referentes a la conducta delictiva de Smishing,				

Tabla 10: *Tipificación alterna al Smishing.*

Pregunta N° 10: ¿Cómo tipificó usted la conducta delictiva del Smishing?				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**
Fueron tipificados como delito de estafa y de	Dos de ellas las tipifique como delito de Estafa y dos	Fueron tipificadas dos como estafa simple y dos	Tipifique como delito de Estafa cuatro carpetas	Fueron tipificadas como Estafa.

manera general como delitos contra el patrimonio.	como Estafa Agravada, una de ellas conforme al numeral 5 del artículo 196-A y el otro con el numeral 6 del artículo 196-A del Código Penal.	como estafa agravada.	fiscales y como Estafa Agravada las dos carpetas restantes.	
Interpretación: Los participantes señalaron que tipificaron la conducta delictiva de Smishing en su mayoría como delito de Estafa o Estafa Agravada, por ser una conducta similar a la conducta típica desplegada.				

Tabla 11: *Estado procesal de los casos de Smishing.*

Pregunta N° 11: ¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Smishing?				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**
Dos carpetas fiscales se encuentran en investigación preliminar, tres carpetas fueron sobreseídas y una pasó a la etapa de acusación.	Dos de las carpetas tipificadas como delito de Estafa fueron archivadas y las otras dos han sido declaradas complejas en preliminar.	Una he formalizado y declarado compleja, mientras que las otras tres fueron archivadas en etapa preliminar.	Cuatro carpetas fiscales fueron archivadas preliminarmente, una carpeta fue sobreseída y la otra llego a etapa de juzgamiento para posteriormente haberse obtenido una sentencia.	Dos de las carpetas fueron archivadas preliminarmente mientras que las otras dos han sido sobreseídas.
Interpretación: Los participantes afirmaron que las carpetas fiscales en su mayoría fueron archivadas o sobreseídas; sin embargo, una cantidad reducida fue formalizada dando continuidad a la investigación.				

Tabla 12: *Incorporación específica de Smishing.*

Pregunta N° 12: ¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Smishing? ¿Por qué?

Entrevistado 01	Entrevistado 02	Entrevistado 03	Entrevistado 04	Entrevistado 05
Considero que, si debe regularse, porque de esa manera los fiscales podríamos enmarcar de una forma adecuada tal delito.	Si, para poder calificar las conductas delictivas con un tipo penal más adecuado.	Si debería de incorporarse porque permite enmarcar específicamente en un delito.	Considero que debería incorporarse puesto que se llegaría a obtener una sentencia con un tipo penal adecuado.	Si por que un tipo penal especifico permitirá que las carpetas puedan formalizarse y no generar impunidad.
Interpretación: La totalidad de participantes expresaron su conformidad para incorporar un tipo penal específico con la finalidad de enmarcar adecuadamente y sancionar la conducta delictiva del Smishing.				

Finalmente, referente al **tercer objetivo específico:** Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Vishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021. Se realizó las siguientes preguntas:

Tabla 13: *Casos referentes al Vishing.*

Pregunta N° 13: ¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Vishing? De ser afirmativa su respuesta, especifique la cantidad.				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**
Se me presentaron aproximadamente diez a once casos de Vishing.	Si he tenido un caso.	Si tuve siete casos de los cuales uno fue acumulado a otra carpeta fiscal.	A lo largo de mi carrera fiscal tuve ocho casos referidos al Vishing.	Tuve seis casos.
Interpretación: La mayoría de los participantes afirmaron haber tenido entre seis y diez casos, mientras que uno de los participantes solo tuvo un caso referente a la conducta delictiva de Vishing a lo largo de su carrera fiscal.				

Tabla 14: *Tipificación alterna de Vishing.*

Pregunta N° 14: ¿Cómo tipificó usted la conducta delictiva del Vishing?

Entrevistado 01	Entrevistado 02	Entrevistado 03	Entrevistado 04	Entrevistado 05
Todas fueron tipificadas como delitos de estafa agravada, establecida en el artículo 196-A numeral 5 del Código Penal.	Se apertura investigación en el cual se tipifico de manera genérica en Delitos Contra el Patrimonio.	Las he tipificado como estafa.	Fueron tipificadas como Estafa Agravada.	Fueron tipificadas como delito de Estafa Agravada.
Interpretación: Los participantes en su totalidad tipificaron la conducta delictiva del Vishing como Delitos Contra el Patrimonio, en la modalidad de Estafa y Estafa Agravada.				

Tabla 15: *Estado procesal de los casos de Vishing.*

Pregunta N° 15: ¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Vishing?				
Entrevistado 01	**Entrevistado 02**	**Entrevistado 03**	**Entrevistado 04**	**Entrevistado 05**
Tres carpetas fiscales fueron formalizadas, cinco carpetas se archivaron en etapa preliminar, una carpeta fue sobreseída y una se encuentra en ejecución de sentencia.	La carpeta fiscal fue archivada en etapa preliminar.	Una carpeta ya está formalizada, una en investigación preparatoria y cuatro archivadas.	Dos carpetas discales fueron declaradas completas después de ser formalizadas y seis carpetas fiscales en etapa preliminar se archivaron.	Fueron sobreseídas por no haberse reunido los elementos de convicción suficientes para imputar delito.
Interpretación: Los entrevistados especificaron que una gran parte de las carpetas fiscales fueron archivadas e incluso sobreseídas, con una menor cantidad de ellas siendo formalizadas.				

Tabla 16: *Incorporación específica de Vishing.*

Pregunta N° 16: ¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Vishing? ¿Por qué?

Entrevistado 01	Entrevistado 02	Entrevistado 03	Entrevistado 04	Entrevistado 05
Considero que se debe regular ya que al tener un tipo penal específico esta conducta seria sancionada de manera correcta y efectiva.	Si, por que al tener una regulación especial o específica, dicha conducta podría ser sancionada.	Si se debería porque permite sancionar los delitos de manera eficiente.	Considero que si deberían incorporarse por cuanto al no existir regulación específica se genera impunidad.	Si debe incorporarse para poder formalizar las carpetas fiscales y sancionar tal conducta.
Interpretación: El total de los entrevistados coincidieron en que si se debería incorporar un tipo penal específico, pues ello permitiría imputar el delito de manera más efectiva.				

Discusión:

Continuando con el capítulo en mención, pasaremos al ámbito de la discusión, que serán presentados en virtud a cada objetivo de la investigación:

En consecuencia, se obtuvo de los resultados que las denuncias de delitos informáticos en los despachos fiscales incrementaron en el periodo 2020 al 2021; es decir, como menciona el autor Ribero (2016) en estos tiempos los delitos informáticos van en incremento debido a que el avance de la tecnología genera diversas y nuevas formas de cometer ilícitos penales, razón por la cual las normas que regulan este tipo de delitos deben avanzar en la misma medida, caso contrario estos delitos seguirán generando millonarias pérdidas. Asimismo, los autores Bokovnya et al (2020) manifiestan que si bien existe una regulación de delitos informáticos; sin embargo, el número de víctimas va en incremento en el tiempo, debido a que las personas se encuentran en constante uso de la tecnología.

Por ende, el avance y uso de la tecnología en épocas actuales ocasiono que muchos de los delincuentes generen nuevas modalidades y formas de cometes delitos, por lo que se ha visto incrementado los casos de delitos informáticos.

De igual forma, se evidencio de los resultados que existe impunidad en nuestro país debido a que las nuevas modalidades del delito informático no cuentan con una regulación específica; por lo que, estas nuevas modalidades deberían regularse en

una ley específica o en el Código Penal, a fin de ser sancionadas. En otras palabras, como señalan los autores Hildalgo y Solano (2021), se ha generado impunidad ya que los tipos penales del Código y la Ley de Delitos Informáticos son deficientes por cuanto no subsumen ni permiten subsumir las nuevas modalidades de delito informático, siendo necesario crear tipo penal específico.

Es por ello, que las nuevas modalidades del delito informático deben ser incorporadas dentro de la legislación peruana dentro de la Ley de Delitos Informáticos, a fin de sancionar las nuevas conductas delictivas que en el país se generan tras el avance tecnológico.

Por otro lado, los resultados muestran que se da la existencia de casos referentes a la conducta delictiva del Phishing a nivel fiscal, conducta que de acuerdo a la investigación fiscal en su mayoría son tipificados como delito de Estafa, Estafa Agravada o de manera genérica como Delitos Contra el Patrimonio, los cuales generalmente tiene como último estado procesal el archivo preliminar, por tal razón, debería regularse como un tipo penal específico. Así pues, el autor Montaño (2019) sostiene que si bien las nuevas modalidades del delito informático se encuentran vinculadas con el delito de Estafa, dado que el objetivo que persigue es el beneficio económico; empero, se diferencia de los delitos informáticos por el medio utilizado (la informática, tecnología, etc.), razón esencial para incorporarlo como tipo penal independiente.

Además, cabe resaltar que el Phishing al ser una conducta que a través del empleo de medios tecnológicos remite correos masivos de información fraudulenta, tiene la finalidad de obtener información personal de la víctima para finalmente obtener un provecho económico.

Asimismo, se obtuvo como resultado, que a lo largo de las investigaciones fiscales realizadas por los fiscales penales de la ciudad de Huaraz, se presentaron casos referentes al Smishing, los cuales fueron tipificados en su mayoría como delito de Estafa o Estafa Agravada, por ser una conducta similar a la conducta típica desplegada; empero, dichos casos en su mayoría fueron archivadas o sobreseídas; sin embargo, una cantidad reducida fue formalizada dando continuidad a la investigación, por lo que se sugiere la incorporación de un tipo penal especifico con la finalidad de enmarcar adecuadamente y sancionar la conducta delictiva del

Smishing. No obstante, debe tenerse en cuenta que el Smishing se diferencia de la Estafa por cuanto como señala el autor Paiva (2021) en este tipo de modalidad se usa un canal de comunicación distinto, ya que se produce usando la tecnología por medio del envío de SMS al celular del usuario mediante una suplantación de identidad que le genera confianza, con la intención de adquirir mayores datos del usuario, siendo la única similitud la obtención de un beneficio económico.

Es por ello, que dicha conducta al ser tipificada como delito de Estafa en la mayoría de los casos es archivado no prosiguiendo con la investigación por cuanto no existe una regulación específica mediante la cual se pueda llegar a sancionar adecuadamente estos ilícitos, enmarcando todos los elementos del tipo penal.

Por otra parte, de los resultados se obtuvo que las investigaciones fiscales respecto a la conducta delictiva de Vishing son tipificadas como Delitos Contra el Patrimonio en su modalidad de Estafa y Estafa Agravada, siendo su ultimo estado procesal el archivo o sobreseimiento, motivo por el cual se debe incorporar un tipo penal específico, pues ello permitiría imputar el delito de manera más efectiva. En otras palabras, como afirma el autor Fuentes (2021) la norma es deficiente en cuanto a la tipificación de las nuevas modalidades del delito informático, debido a que la Ley de Delitos Informáticos solo se encarga de regular de manera genérica el medio por el que se comete un ilícito informático más no la conducta específica.

De allí, que en las investigaciones fiscales ante la inexistencia de un tipo penal especifico de Vishing, se tipifica como Delitos Contra el Patrimonio, pese a que es un delito informático y el medio que se utiliza al respecto es la tecnología.

V. CONCLUSIONES

PRIMERO.- Las nuevas modalidades del delito informático se han desarrollado a la par del avance de la tecnología; es decir, estas son consecuencia de un desarrollo constante de la tecnología, es así que se convierte en una necesidad la regulación de conductas repudiadas por un Estado Constitucional. El cuerpo legal específico para regular dichas conductas es la Ley N° 30096 y la Ley N° 30171 que modifica la misma, siendo esta Ley de Delitos Informáticos dirigida a sancionar aquellos actos ilícitos que se cometen con el uso de medios tecnológicos, puesto que las normas específicas regulan las conductas que son recurrentes en el

accionar delictivo, es así que teniendo en cuenta lo mencionado por los fiscales del Ministerio Público en la entrevista se infiere que los casos de Phishing, Smishing y Vishing van en incremento, por ende, la ley debe incorporar estas modalidades como conductas específicas, con el objetivo que lleguen a ser sancionadas.

SEGUNDO.- Ante la usencia de un tipo penal específico del Phishing las investigaciones fiscales referentes a esta conducta delictiva son desarrolladas o tipificadas como delitos contra el patrimonio generalmente enmarcadas en la modalidad de Estafa Simple o Agravada, por lo que en mucho de los casos llegan a ser archivadas por no tener un tipo penal adecuado que enmarque de forma correcta los elementos típicos del Phishing, tales como sujeto activo (phisher) y pasivo (víctima), verbo rector (enviar), conducta delictiva (envío de correo electrónico fraudulento), bien jurídico protegido (la confidencialidad de la información y el patrimonio).

TERCERO.- La conducta delictiva del Smishing, en el contexto nacional tiende a ser frecuente, puesto que un gran porcentaje de la población cuenta con aplicativos de mensajería, medio idóneo que permite la comisión del acto ilícito, es por ello que ante las denuncias remitida a los diferentes despachos de la Fiscalía Penal Corporativa de Ancash, los Fiscales deben de adecuar las imputaciones relacionadas al Smishing, tipificando como delitos como Estafa Simple o Agravada; generando que la mayoría de las carpetas fiscales fueran archivadas o sobreseídas y un mínimo de carpetas fiscales puedan ser formalizadas como delito de Estafa, no teniendo en cuenta los elementos típicos del delito como sujeto activo (smisher) y pasivo (receptor o víctima), verbo rector (enviar y aprovechar), conducta delictiva (envío de mensaje o SMS maliciosos), bien jurídico protegido (información personal, datos confidenciales y patrimonio).

CUARTO.- La conducta delictiva del Vishing es una modalidad que se generó a partir de la popularidad del uso de dispositivos móviles, debido a que se configura mediante llamadas telefónicas utilizando la suplantación de identidad para obtener la información de la víctima, generalmente estos casos son investigados por la Fiscalía Penal Corporativa de Ancash como delitos contra el patrimonio, mas no como delitos informáticos de manera específica razón por la cual en su mayoría son archivadas e incluso sobreseídas, sin tener en cuenta los elementos típicos

para cada caso en concreto en los cuales encontramos: sujeto activo (visher) y pasivo (usuario o víctima), verbo rector (llamar y aprovechar), conducta delictiva (realizar llamadas suplantando la identidad), bien jurídico protegido (seguridad informática, información confidencial y patrimonio). Por lo que, se considera necesario su incorporación dentro de la Ley de Delitos Informáticos, con el propósito de evitar la impunidad.

VI. RECOMENDACIONES

PRIMERO.- Se recomienda a los legisladores peruanos regular las nuevas modalidades del delito informático como tipos penales específicos, correspondientes a las conductas delictivas del Phishing, Smishing y Vishing, dentro de la Ley de Delitos Informáticos Ley N° 30096 y la Ley N° 30171 que modifica la misma.

SEGUNDO: Se recomienda al Fiscal de la Nación y al Presidente del Poder Judicial buscar regular las nuevas modalidades del delito informático correspondientes a las conductas delictivas del Phishing, Smishing y Vishing, como conductas especificas dentro de la Ley de Delitos Informáticos, en virtud al derecho de iniciativa legislativa.

TERCERO.- Se recomienda al Ministerio Público capacitar al personal fiscal sobre temas de Delitos Informáticos; asimismo, replicar esas capacitaciones en las instituciones públicas que trabajan a la par, tales como la Policía Nacional del Perú, Procuraduría pública, Ministerio de Justicia, entre otros.

CUARTO.- Se recomienda al Ministerio Público instaurar Fiscalías Especializadas en Delitos Informáticos en los distritos fiscales a nivel nacional con la finalidad de afrontar de manera eficaz y organizada contra la ciberdelincuencia.

REFERENCIAS

1. Acosta, M.G., Benavides, M.M. & García, N.P. (2020). Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios. *Revista Venezolana de Gerencia, 25(89),* 351–368.
2. Altwairqi, A. F., AlZain, M. A., Soh, B., Masud, M., & Al-Amri, J. (2019). Four most famous cyber-attacks for financial gains. Int. J. Eng. Adv. Technol, 9, 2131-2139.
3. Banire, B., Al Thani, D., & Yang, Y. (2021, julio). Abordar la accesibilidad a la seguridad cibernética: un estudio cualitativo. En 34th British HCI Workshop and Doctoral Consortium 34 (pp. 1-5).
4. Bokovnya, A. Y., Khisamova, Z. I., Begishev, I. R., Latypova, E. Y., & Nechaeva, E. V. (2020). Computer crimes on the COVID-19 scene: analysis of social, legal, and criminal threats. Cuestiones Políticas, 38(66), 463-472.
5. Código Penal [CP]. Decreto Legislativo N.º 635. 03 de abril de 1991. Recuperado de https://spij.minjus.gob.pe/spij-ext-web/detallenorma/H682692
6. Código Penal Alemán. del 15 de mayo de 1871. Traducido por López Diaz, C. Recuperado de https://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20080616_02.pdf
7. Código Penal Colombiano. Ley 599 de 2000. Diario Oficial N° 44.097 de 24 de julio de 2000. Última actualización: 31 de agosto de 2022 - (Diario Oficial No. 52143 - 31 de agosto de 2022). Recuperado de http://www.secretariasenado.gov.co/senado/basedoc/ley_0599_2000.html
8. Código Penal de la Nación de Argentina. Ley 11.179. Texto Ordenado por Decreto 3992/84 de 21 de diciembre de 1984. Recuperado de http://servicios.infoleg.gob.ar/infolegInternet/anexos/15000-19999/16546/texact.htm
9. Código Penal Español. Ley Orgánica 5/2010, de 22 de junio, por la que se modifica la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal Español. Recuperado de https://noticias.juridicas.com/base_datos/Penal/lo10-1995.l2t13.html#a248

10. Devia González, E.A. (2017). El delito informático: Estafa informática del Artículo 248.2 del Código Penal. (Tesis Doctoral Inédita). Universidad de Sevilla, Sevilla. https://hdl.handle.net/11441/75625
11. Díaz Quezada, J., & Hernández Bejarano, M. (2021). Amenazas a la información personal financiera. *Revista Avenir, 5(1),* 16-23. Recuperado a partir de https://fundacionavenir.net/revista/index.php/avenir/article/view/111
12. Esparta Centero, M. M. (2022) *Mecanismos de prevención y protección del bien jurídico tutelado frente a la modalidad delictiva Phishing en el ordenamiento jurídico penal peruano* [Tesis de Grado, Universidad Inca Garcilaso de la Vega]. http://repositorio.uigv.edu.pe/handle/20.500.11818/6595
13. Fuentes Garrido, K. V. (2021). *Modificación de la Ley 30096 para incorporar los delitos de phishing, pharming y carding como delitos penalizables con prisión, para reducir la ciberdelincuencia, Lima 2019* [Tesis de Grado, Universidad Señor de Sipán]. https://repositorio.uss.edu.pe/handle/20.500.12802/8345
14. García Forero, L. F. G. (2020). *Ciberseguridad en las organizaciones, el personal potencial fuente de riesgo.* [Tesis de grado. Universidad Piloto de Colombia]. http://repository.unipiloto.edu.co/handle/20.500.12277/9545
15. García García, D. E. (2018). El Phishing como delito de estafa informática. Comentario a la SAP de Valencia 37/2017 de 25 de enero (rec. 1402/2016). *Iuris Tantum Revista Boliviana de Derecho*, (25), 650-661.
16. Gonzáles, J., Bermeo, J., Villacreses, E., & Guerrero, J. (2018, July). Delitos informáticos: una revisión en Latinoamérica. In Conference Proceedings UTMACH (Vol. 2, No. 1).
17. Guevara Alban, G. P., Verdesoto Arguello, A. E., & Castro Molina, N. E. (2020). Metodologías de investigación educativa (descriptivas, experimentales, participativas, y de investigación-acción). RECIMUNDO, 4(3), 163-173.
18. Hernández, R., Fernández, C., & Baptista, P. (2016). Metodología de la investigación. 6ta Edición Sampieri. *Soriano, RR (1991). Guía para realizar investigaciones sociales. Plaza y Valdés*.
19. Hidalgo Coronel, C. N., y Solano Vidal, G. S. (2021). *El phishing como conducta delictiva no regulada en el ordenamiento jurídico peruano. Propuesta de incorporación del artículo 7-a en la Ley de Delitos Informáticos 30096.* [Tesis de

Grado, Universidad Nacional del Santa]. http://repositorio.uns.edu.pe/handle/UNS/3849

20. Kalaharsha, P., & Mehtre, B. M. (2021). Detecting Phishing Sites - An Overview. arXiv preprint arXiv:2103.12739. https://doi.org/10.48550/arXiv.2103.12739
21. Ley N° 30171 de 2014. Ley que modifica la Ley 30096, Ley de Delitos Informáticos. 10 de marzo de 2014. https://spij.minjus.gob.pe/spij-ext-web/detallenorma/H1097704
22. Ley Nº 30096 de 2013. Ley de Delitos Informáticos. 22 de octubre de 2013. Recuperado de https://spij.minjus.gob.pe/spij-ext-web/detallenorma/H1088463
23. Mayer Lux, Laura, & Oliver Calderón, Guillermo. (2020). El delito de fraude informático: concepto y delimitación. Revista chilena de derecho y tecnología, 9(1), 151-184. https://dx.doi.org/10.5354/0719-2584.2020.53447
24. Medina Martínez, J. J., Cárdenas Osorio, C. H. y Mejía Lobo, M. (2021). *Análisis del Phishing y la Ley de delitos informáticos en Colombia.* Cuaderno de investigaciones: semilleros andina, 1(14).
25. Mishra, Sandhya., y Soni, Devpriya (2020). Smishing Detector: A security model to detect smishing through SMS content analysis and URL behavior analysisFuture Generation Computer Systems, 108(), 803–815.
26. Montaño Mamani, R. (2019). *La tipificación penal del phishing, como medida de seguridad informática para contener delitos informáticos.* [Tesis de Grado, Universidad Mayor de San Andrés].
27. Njuguna, D. N. ., Kamau, J. ., & Kaburu, D. . (2022). A Review of Smishing Attaks Mitigation Strategies. Revista Internacional de Informática y Tecnología de la Información (2279-0764),11(1). https://doi.org/10.24203/ijcit.v11i1.201
28. Oficina de Análisis Estratégico Contra la Criminalidad – OFAEC. (2021) *Informe de Análisis N°04 Ciberdelincuencia: Pautas para una investigación fiscal especializada oficina de análisis estratégico contra la criminalidad.* Ministerio Público. Fiscalía de la Nación. Recuperado de https://www.gob.pe/institucion/mpfn/informes-publicaciones/1667473-ciberdelincuencia-en-el-peru-pautas-para-su-investigacion-fiscal-especializada
29. Oficina de las Naciones Unidas contra la Droga y el Delito - UNODC. (2020) *Guía Didáctica para Docentes. Serie de Módulos Universitarios.*

Ciberdelincuencia. Educación para la Justicia Recuperado de https://www.unodc.org/e4j/es/tertiary/cybercrime.html

30. Paiva Murcia, R. (2021). *El paradigma objetivo en la responsabilidad de las entidades bancarias por fraude electrónico: una mirada desde las obligaciones de resultado.* [Tesis de Maestría, Universidad Nacional de Colombia].
31. Parada, R. A., y Errecaborde, J. D. (2018). *Cibercrimen y delitos informáticos: los nuevos tipos penales en la era de internet.* Buenos Aires: Erreius.
32. Paredes Vargas, C. L. (2021). Oportunidades de mejora detrás de la principal preocupación del sistema financiero: fraudes informáticos. Seminario de Grado Universidad Militar Nueva Granada Facultad de Estudios a Distancia Especialización en Alta Gerencia Bogotá, Colombia. http://hdl.handle.net/10654/39412
33. Pimienta Prieto, J. H. & De la Orden Hoz A. (2017). Metodología de la Investigación Científica. Tercera Edición. Pearson Educación. Sede Académica La Paz.
34. Pons Gamón, V. (2017). Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. URVIO - Revista Latinoamericana de Seguridad Ciudadana, 20, 80–93. https://doi.org/10.17141/urvio.20.2017.2563
35. Ribero Corzo, S. M. (2016) *Delitos Informáticos y su legislación en el contexto Colombiano. Retos Sociales y Tecnológicos Nacionales* [Tesis de Grado, Universidad Autónoma de Bucanamarca]. https://repository.unab.edu.co/handle/20.500.12749/1305
36. Salvi, M. (2019) *El Phishing en la Argentina* [Tesis de Grado, Universidad Siglo 21]. https://repositorio.uesiglo21.edu.ar/handle/ues21/16066
37. Sequeiros Calderon, I. C. (2016) *Vacíos legales que imposibilitan la sanción de los delitos informáticos en el Nuevo Código Penal Peruano – 2015* [Tesis de Grado, Universidad de Huánuco]. http://repositorio.udh.edu.pe/123456789/286
38. Tacilio Yauli, E. F. (2016). Metodología de la Investigación Científica. Universidad Jaime Bausate y Meza. Recuperado de http://repositorio.bausate.edu.pe/handle/bausate/36

39. Tóala, G. M. T., y Briones, A. A. M. (2019). Importancia de la enseñanza de la metodología de la investigación científica en las ciencias administrativas. Dominio de las Ciencias, 5(2), 56-70.
40. Trávez Carrasco, N. (2019). *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).* [Tesis de Grado, Universidad Central de Ecuador]. http://www.dspace.uce.edu.ec/handle/25000/18733
41. Ventura, M. A. (2021). *La tipificación del phishing, smishing y vishing en nuestro sistema penal peruano, para la lucha contra la ciberdelincuencia en Lima, 2020* [Tesis de licenciatura, Universidad Privada del Norte]. https://hdl.handle.net/11537/28942
42. Vilca Aira, G. L. (2018) *Los Hackers: "Delito Informático frente al Código Penal Peruano* [Tesis de Grado, Universidad Santiago Antúnez de Mayolo]. http://repositorio.unasam.edu.pe/handle/UNASAM/2496
43. 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, (E17),* 671-677.

ANEXOS

Anexo 01: Matriz de categorización

<table>
<tr><th>PROBLEMAS</th><th>OBJETIVOS</th><th>AMBITO TEMÁTICO</th><th>CATEGORIAS</th><th>SUBCATEGORIAS</th><th>METODOLOGÍA</th></tr>
<tr><td>GENERAL</td><td>GENERAL</td><td rowspan="5">NUEVAS MODALIDADES DEL DELITO INFORMÁTICO</td><td rowspan="2">PHISHING</td><td rowspan="2">• Web y correos electrónico
• Sujetos
• Conducta
• Bien jurídico protegido</td><td rowspan="5">ENFOQUE DE INVESTIGACIÓN
Cualitativo

TIPO DE INVESTIGACIÓN
Aplicada

NIVEL DE INVESTIGACIÓN
Descriptivo

DISEÑO DE INVESTIGACIÓN
Teoría Fundamentada</td></tr>
<tr><td>¿De qué manera la Ley N° 30096 y su modificatoria Ley N° 30171 regularían las nuevas modalidades del delito informático en el periodo 2020-2021?</td><td>Fundamentar la regulación de las nuevas modalidades del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171</td></tr>
<tr><td>ESPECÍFICO</td><td>ESPECÍFICO</td><td rowspan="2">SMISHING</td><td rowspan="2">• SMS o mensajes
• Sujetos
• Conducta
• Bien jurídico protegido</td></tr>
<tr><td>PE1: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Phishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?</td><td>OE1: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Phishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021</td></tr>
<tr><td>PE2: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Smishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?</td><td>OE2: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Smishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021</td><td>VISHING</td><td>• Voz o llamadas telefónicas
• Sujetos
• Conducta
• Bien jurídico protegido</td></tr>
<tr><td>PE3: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Vishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?</td><td>OE3: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Vishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021</td></tr>
</table>

Anexo 02: Instrumento de recolección de datos

GUÍA DE ENTREVISTA

TÍTULO: "La Regulación de las Nuevas Modalidades del Delito Informático en la Ley N° 30096 y su Modificatoria, periodo 2020-2021."

AUTORES : RAMOS CALDUA MIRIAN CATY
SALVADOR ROJAS YORMAN ANDREY

Entrevistado (a) : _____

Profesión o Cargo: _____

Institución : _____

La presente entrevista tiene como finalidad recopilar información a fin de un posterior análisis y desarrollo de la investigación; razón por la cual, usted como participante deberá responder las siguientes preguntas.

AMBITO TEMÁTICO: NUEVAS MODALIDADES DEL DELITO INFORMÁTICO.

1. ¿Usted recibió charlas informativas, capacitaciones o cursos especializados en delitos informáticos, ofrecidas por el Ministerio Público u otra entidad? Precise.

   _____

   _____

   _____

2. ¿Durante el periodo 2020 al 2021 las denuncias en su despacho respecto a delitos informáticos incrementaron? De ser afirmativa su respuesta precise ¿Por qué?

   _____

   _____

   _____

   _____

3. ¿La falta de regulación específica de las nuevas modalidades del delito informático generan impunidad? ¿Por qué?

   _____

   _____

_____

_____

4. ¿Considera que las nuevas modalidades del delito informático deberían encontrarse reguladas en la Ley Nro. 30096, su modificatoria Ley N° 30171 o en el Código Penal? ¿Por qué?

_____

_____

_____

_____

CATEGORÍA 01: PHISHING

5. ¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Phishing? De ser afirmativa su respuesta, especifique la cantidad.

_____

_____

_____

6. ¿Cómo tipificó usted la conducta delictiva del Phishing?

_____

_____

_____

_____

7. ¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Phishing?

_____

_____

_____

_____

8. ¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Phishing? ¿Por qué?

_____

_____

_____

_____

CATEGORIA 02: SMISHING

9. ¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Smishing? De ser afirmativa su respuesta, especifique la cantidad.

_____

_____

_____

10. ¿Cómo tipificó usted la conducta delictiva del Smishing?

_____

_____

_____

_____

11. ¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Smishing?

_____

_____

_____

_____

12. ¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Smishing? ¿Por qué?

_____

_____

_____

_____

CATEGORIA 03: VISHING

13. ¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Vishing? De ser afirmativa su respuesta, especifique la cantidad.

_____

_____

_____

14. ¿Cómo tipificó usted la conducta delictiva del Vishing?

_____

_____

_____

_____

15. ¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Vishing?

_____

_____

_____

_____

16. ¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Vishing? ¿Por qué?

_____

_____

_____

_____

_____

Firma

Anexo 03: Certificado de validez de intrumento

UNIVERSIDAD CÉSAR VALLEJO *FACULTAD DE DERECHO Y HUMANIDADES*

CARTA DE PRESENTACIÓN

Huaraz, 27 de setiembre de 2022.

Mag. ROBERT ALEXANDER ROJAS ASCÓN

Presente.

ASUNTO: Participación en juicio de expertos para validar instrumento de investigación cualitativa.

Nos es grato dirigirnos a usted para expresarle nuestros saludos y a la vez solicitarle su colaboración como experto en la presente investigación lleva por título "LA REGULACIÓN DE LAS NUEVAS MODALIDADES DEL DELITO INFORMÁTICO EN LA LEY N° 30096 Y SU MODIFICATORIA, PERIODO 2020-2021" conducida por los estudiantes Ramos Caldua Mirian Caty y Salvador Rojas Yorman Andrey, investigación que servirá para obtener el título profesional de Abogado.

Razón por la cual, a fin de contar con el rigor científico necesario, se requiere la validación del instrumento de recolección de datos; por lo que, solicitamos su participación como juez conocedor y experto, a colaborar con la presente investigación, apelando su trayectoria y reconocimiento como docente universitario y profesional, para validar el instrumento correspondiente a una guía de entrevista, que cuenta con 16 preguntas, el cual será aplicado a 5 Fiscales de las Fiscalías Provinciales Penales Corporativas de Huaraz, con la finalidad recoger información directa para la investigación, cuyas preguntas deben ser validados por expertos, por lo que, solicito a usted como conocedor y experto validar el presente instrumento.

Asimismo, para efectuar la validación del instrumento, el validador deberá leer cada enunciado y las alternativas de respuesta. Por otra parte, se le agradece cualquier sugerencia que considere ayude a la mejora de la presente investigación.

Se adjunta al presente expediente de validación, lo siguiente:

- Carta de presentación
- Matriz de categorización

- Certificado de validez de instrumento

Sin otro particular, aprovechamos la ocasión para renovarle las muestras de nuestra distinguida consideración y estima, agradeciendo anticipadamente su colaboración y aporte en la presente investigación.

Atentamente,

MIRIAN CATY RAMOS CALDUA
DNI N° 70567840

YORMAN ANDREY SALVADOR ROJAS
DNI N° 72500229

MATRIZ DE CATEGORIZACIÓN

PROBLEMAS	OBJETIVOS	AMBITO TEMÁTICO	CATEGORIAS	SUBCATEGORIAS	METODOLOGÍA
GENERAL	**GENERAL**	**NUEVAS MODALIDADES DEL DELITO INFORMÁTICO**	PHISHING	• Web y correos electrónico • Sujetos • Conducta • Bien jurídico protegido	**ENFOQUE DE INVESTIGACIÓN** Cualitativo **TIPO DE INVESTIGACIÓN** Aplicada **NIVEL DE INVESTIGACIÓN** Descriptivo **DISEÑO DE INVESTIGACIÓN** Teoría Fundamentada
¿De qué manera la Ley N° 30096 y su modificatoria Ley N° 30171 regularían las nuevas modalidades del delito informático en el periodo 2020-2021?	Fundamentar la regulación de las nuevas modalidades del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171				
ESPECÍFICO	**ESPECÍFICO**		SMISHING	• SMS o mensajes • Sujetos • Conducta • Bien jurídico protegido	
PE1: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Phishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?	OE1: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Phishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021				
PE2: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Smishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?	OE2: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Smishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021		VISHING	• Voz o llamadas telefónicas • Sujetos • Conducta • Bien jurídico protegido	
PE3: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Vishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?	OE3: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Vishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021				

CERTIFICADO DE VALIDEZ DE INSTRUMENTO

Instrucciones: Señor (a) especialista se le solicita su colaboración a fin de que posterior al análisis del presente instrumento, proceda a marcar con un aspa (X) según corresponda, de acuerdo a su criterio y experiencia profesional.

TÍTULO: LA REGULACIÓN DE LAS NUEVAS MODALIDADES DEL DELITO INFORMÁTICO EN LA LEY N° 30096 Y SU MODIFICATORIA, PERIODO 2020-2021										
N.°	CATEGORIAS	Pertinencia		Relevancia		Claridad		Suficiencia		Sugerencias
	AMBITO TEMÁTICO: LAS NUEVAS MODALIDADES DEL DELITO INFORMÁTICO	Si	No	Si	No	Si	No	Si	No	
1	¿Usted recibió charlas informativas, capacitaciones o cursos especializados en delitos informáticos, ofrecidas por el Ministerio Público u otra entidad? Precise.	X		X		X				
2	¿Durante el periodo 2020 al 2021 las denuncias en su despacho respecto a delitos informáticos incrementaron? De ser afirmativa su respuesta precise ¿Por qué?	X		X		X		X		
3	¿La falta de regulación específica de las nuevas modalidades del delito informático generan impunidad? ¿Por qué?	X		X		X				
4	¿Considera que las nuevas modalidades del delito informático deberían encontrarse reguladas en la Ley Nro. 30096, su modificatoria Ley N° 30171 o en el Código Penal? ¿Por qué?	X		X		X				

CATEGORIA 01: PHISHING		Pertinencia		Relevancia		Claridad		Suficiencia		Sugerencias
SUBCATEGORIAS: Web y correos electrónico, sujetos, conducta y bien jurídico protegido		Si	No	Si	No	Si	No	Si	No	
5	¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Phishing? De ser afirmativa su respuesta, especifique la cantidad.	X		X		X		X		
6	¿Cómo tipificó usted la conducta delictiva del Phishing?	X		X		X				
7	¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Phishing?	X		X		X				
8	¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Phishing? ¿Por qué?	X		X		X				
CATEGORÍA 02: SMISHING		Pertinencia		Relevancia		Claridad		Suficiencia		Sugerencias
SUBCATEGORIAS: SMS o mensajes, sujetos, conducta y bien jurídico protegido		Si	No	Si	No	Si	No	Si	No	
09	¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Smishing? De ser afirmativa su respuesta, especifique la cantidad.	X		X		X		X		

10	¿Cómo tipificó usted la conducta delictiva del Smishing?	X		X		X				
11	¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Smishing?	X		X		X		X		
12	¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Smishing? ¿Por qué?	X		X		X				
CATEGORÍA 03: VISHING		**Pertinencia**		**Relevancia**		**Claridad**		**Suficiencia**		**Sugerencias**
SUBCATEGORIAS: Voz o llamadas telefónicas, sujetos, conducta y bien jurídico protegido		**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Vishing? De ser afirmativa su respuesta, especifique la cantidad.	X		X		X				
14	¿Cómo tipificó usted la conducta delictiva del Vishing?	X		X		X		X		
15	¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Vishing?	X		X		X				
16	¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Vishing? ¿Por qué?	X		X		X				

Observaciones: _____

_____

_____

Opinión de aplicabilidad:

- Aplicable [X]
- Aplicable después de corregir [ ]
- No aplicable [ ]

DATOS DEL JUEZ EXPERTO VALIDADOR

Apellidos y nombres : ROBERT ALEXANDER ROSAS ASCÓN

DNI N° : 42556042

Profesión : ABOGADO

Especialidad : PENAL – MAGISTER EN DERECHO PENAL

Cargo : FISCAL PROVINCIAL

Institución : MINISTERIO PÚBLICO

Huaraz, 27 de SETIEMBRE del 2022.

ROBERT ALEXANDER ROJAS ASCÓN
FISCAL PROVINCIAL DEL DESPACHO TRANSITORIO
DE LA FISCALÍA PROVINCIAL CORPORATIVA ESPECIALIZADA
EN DELITOS DE CORRUPCIÓN DE FUNCIONARIOS DEL
DISTRITO FISCAL DE ANCASH.

Firma del experto

CARTA DE PRESENTACIÓN

Huaraz, 27 de setiembre de 2022.

Mag. MARCO ANTONIO ESPINAL BRAVO

Presente.

ASUNTO: Participación en juicio de expertos para validar instrumento de investigación cualitativa.

Nos es grato dirigirnos a usted para expresarle nuestros saludos y a la vez solicitarle su colaboración como experto en la presente investigación lleva por título "LA REGULACIÓN DE LAS NUEVAS MODALIDADES DEL DELITO INFORMÁTICO EN LA LEY N° 30096 Y SU MODIFICATORIA, PERIODO 2020-2021" conducida por los estudiantes Ramos Çaldua Mirian Caty y Salvador Rojas Yorman Andrey, investigación que servirá para obtener el título profesional de Abogado.

Razón por la cual, a fin de contar con el rigor científico necesario, se requiere la validación del instrumento de recolección de datos; por lo que, solicitamos su participación como juez conocedor y experto, a colaborar con la presente investigación, apelando su trayectoria y reconocimiento como docente universitario y profesional, para validar el instrumento correspondiente a una guía de entrevista, que cuenta con 16 preguntas, el cual será aplicado a 5 Fiscales de las Fiscalías Provinciales Penales Corporativas de Huaraz, con la finalidad recoger información directa para la investigación, cuyas preguntas deben ser validados por expertos, por lo que, solicito a usted como conocedor y experto validar el presente instrumento.

Asimismo, para efectuar la validación del instrumento, el validador deberá leer cada enunciado y las alternativas de respuesta. Por otra parte, se le agradece cualquier sugerencia que considere ayude a la mejora de la presente investigación.

Se adjunta al presente expediente de validación, lo siguiente:

- Carta de presentación
- Matriz de categorización

- Certificado de validez de instrumento

Sin otro particular, aprovechamos la ocasión para renovarle las muestras de nuestra distinguida consideración y estima, agradeciendo anticipadamente su colaboración y aporte en la presente investigación.

Atentamente,

MIRIAN CATY RAMOS CALDUA
DNI N° 70567840

YORMAN ANDREY SALVADOR ROJAS
DNI N° 72500229

MATRIZ DE CATEGORIZACIÓN

PROBLEMAS	OBJETIVOS	AMBITO TEMÁTICO	CATEGORIAS	SUBCATEGORIAS	METODOLOGÍA
GENERAL	**GENERAL**	**NUEVAS MODALIDADES DEL DELITO INFORMÁTICO**	PHISHING	• Web y correos electrónico • Sujetos • Conducta • Bien jurídico protegido	**ENFOQUE DE INVESTIGACIÓN** Cualitativo **TIPO DE INVESTIGACIÓN** Aplicada **NIVEL DE INVESTIGACIÓN** Descriptivo **DISEÑO DE INVESTIGACIÓN** Teoría Fundamentada
¿De qué manera la Ley N° 30096 y su modificatoria Ley N° 30171 regularían las nuevas modalidades del delito informático en el periodo 2020-2021?	Fundamentar la regulación de las nuevas modalidades del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171				
ESPECÍFICO	**ESPECÍFICO**		SMISHING	• SMS o mensajes • Sujetos • Conducta • Bien jurídico protegido	
PE1: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Phishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?	OE1: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Phishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021				
PE2: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Smishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?	OE2: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Smishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021		VISHING	• Voz o llamadas telefónicas • Sujetos • Conducta • Bien jurídico protegido	
PE3: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Vishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?	OE3: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Vishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021				

CERTIFICADO DE VALIDEZ DE INSTRUMENTO

Instrucciones: Señor (a) especialista se le solicita su colaboración a fin de que posterior al análisis del presente instrumento, proceda a marcar con un aspa (X) según corresponda, de acuerdo a su criterio y experiencia profesional.

TÍTULO: LA REGULACIÓN DE LAS NUEVAS MODALIDADES DEL DELITO INFORMÁTICO EN LA LEY N° 30096 Y SU MODIFICATORIA, PERIODO 2020-2021										
N.°	CATEGORIAS	Pertinencia		Relevancia		Claridad		Suficiencia		Sugerencias
	AMBITO TEMÁTICO: LAS NUEVAS MODALIDADES DEL DELITO INFORMÁTICO	Si	No	Si	No	Si	No	Si	No	
1	¿Usted recibió charlas informativas, capacitaciones o cursos especializados en delitos informáticos, ofrecidas por el Ministerio Público u otra entidad? Precise.	X		X		X		X		
2	¿Durante el periodo 2020 al 2021 las denuncias en su despacho respecto a delitos informáticos incrementaron? De ser afirmativa su respuesta precise ¿Por qué?	X		X		X				
3	¿La falta de regulación específica de las nuevas modalidades del delito informático generan impunidad? ¿Por qué?	X		X		X				
4	¿Considera que las nuevas modalidades del delito informático deberían encontrarse reguladas en la Ley Nro. 30096, su modificatoria Ley N° 30171 o en el Código Penal? ¿Por qué?	X		X		X				

CATEGORIA 01: PHISHING		Pertinencia		Relevancia		Claridad		Suficiencia		Sugerencias
SUBCATEGORIAS: Web y correos electrónico, sujetos, conducta y bien jurídico protegido		Si	No	Si	No	Si	No	Si	No	
5	¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Phishing? De ser afirmativa su respuesta, especifique la cantidad.	X		X		X		X		
6	¿Cómo tipificó usted la conducta delictiva del Phishing?	X		X		X				
7	¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Phishing?	X		X		X				
8	¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Phishing? ¿Por qué?	X		X		X				
CATEGORÍA 02: SMISHING		Pertinencia		Relevancia		Claridad		Suficiencia		Sugerencias
SUBCATEGORIAS: SMS o mensajes, sujetos, conducta y bien jurídico protegido		Si	No	Si	No	Si	No	Si	No	
09	¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Smishing? De ser afirmativa su respuesta, especifique la cantidad.	X		X		X				

10	¿Cómo tipificó usted la conducta delictiva del Smishing?	X		X		X				
11	¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Smishing?	X		X		X		X		
12	¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Smishing? ¿Por qué?	X		X		X				
CATEGORÍA 03: VISHING		**Pertinencia**		**Relevancia**		**Claridad**		**Suficiencia**		**Sugerencias**
SUBCATEGORIAS: Voz o llamadas telefónicas, sujetos, conducta y bien jurídico protegido		**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Vishing? De ser afirmativa su respuesta, especifique la cantidad.	X		X		X				
14	¿Cómo tipificó usted la conducta delictiva del Vishing?	X		X		X		X		
15	¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Vishing?	X		X		X				
16	¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Vishing? ¿Por qué?	X		X		X				

Observaciones: Ninguna.

Opinión de aplicabilidad:

- Aplicable [X]
- Aplicable después de corregir [ ]
- No aplicable [ ]

DATOS DEL JUEZ EXPERTO VALIDADOR

Apellidos y nombres : ESPINAL BRAVO, MARCO ANTONIO

DNI N° : 30954908

Profesión : ABOGADO

Especialidad : DERECHO PROCESAL PENAL Y LITIGACION ORAL

Cargo : FISCAL PROVINCIAL PENAL TITULAR

Institución : MINISTERIO PÚBLICO

Huaraz, 27 de Setiembre del 2022.

Firma del experto

CARTA DE PRESENTACIÓN

Huaraz, 27 de setiembre de 2022.

Mag. VÍCTOR TÚLLUME PISFIL

Presente.

ASUNTO: Participación en juicio de expertos para validar instrumento de investigación cualitativa.

Nos es grato dirigirnos a usted para expresarle nuestros saludos y a la vez solicitarle su colaboración como experto en la presente investigación lleva por título "LA REGULACIÓN DE LAS NUEVAS MODALIDADES DEL DELITO INFORMÁTICO EN LA LEY N° 30096 Y SU MODIFICATORIA, PERIODO 2020-2021" conducida por los estudiantes Ramos Caldua Mirian Caty y Salvador Rojas Yorman Andrey, investigación que servirá para obtener el título profesional de Abogado.

Razón por la cual, a fin de contar con el rigor científico necesario, se requiere la validación del instrumento de recolección de datos; por lo que, solicitamos su participación como juez conocedor y experto, a colaborar con la presente investigación, apelando su trayectoria y reconocimiento como docente universitario y profesional, para validar el instrumento correspondiente a una guía de entrevista, que cuenta con 16 preguntas, el cual será aplicado a 5 Fiscales de las Fiscalías Provinciales Penales Corporativas de Huaraz, con la finalidad recoger información directa para la investigación, cuyas preguntas deben ser validados por expertos, por lo que, solicito a usted como conocedor y experto validar el presente instrumento.

Asimismo, para efectuar la validación del instrumento, el validador deberá leer cada enunciado y las alternativas de respuesta. Por otra parte, se le agradece cualquier sugerencia que considere ayude a la mejora de la presente investigación.

Se adjunta al presente expediente de validación, lo siguiente:

- Carta de presentación
- Matriz de categorización

- Certificado de validez de contenido y los instrumentos

Sin otro particular, aprovechamos la ocasión para renovarle las muestras de nuestra distinguida consideración y estima, agradeciendo anticipadamente su colaboración y aporte en la presente investigación.

Atentamente,

MIRIAN CATY RAMOS CALDUA
DNI N° 70567840

YORMAN ANDREY SALVADOR ROJAS
DNI N° 72500229

MATRIZ DE CATEGORIZACIÓN

PROBLEMAS	OBJETIVOS	AMBITO TEMÁTICO	CATEGORIAS	SUBCATEGORIAS	METODOLOGÍA
GENERAL	**GENERAL**	**NUEVAS MODALIDADES DEL DELITO INFORMÁTICO**	PHISHING	• Web y correos electrónico • Sujetos • Conducta • Bien jurídico protegido	**ENFOQUE DE INVESTIGACIÓN** Cualitativo **TIPO DE INVESTIGACIÓN** Aplicada **NIVEL DE INVESTIGACIÓN** Descriptivo **DISEÑO DE INVESTIGACIÓN** Teoría Fundamentada
¿De qué manera la Ley N° 30096 y su modificatoria Ley N° 30171 regularían las nuevas modalidades del delito informático en el periodo 2020-2021?	Fundamentar la regulación de las nuevas modalidades del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171				
ESPECÍFICO	**ESPECÍFICO**		SMISHING	• SMS o mensajes • Sujetos • Conducta • Bien jurídico protegido	
PE1: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Phishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?	OE1: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Phishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021				
PE2: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Smishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?	OE2: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Smishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021		VISHING	• Voz o llamadas telefónicas • Sujetos • Conducta • Bien jurídico protegido	
PE3: ¿Cómo se desarrolla alternativamente la investigación fiscal de la conducta delictiva del Vishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021?	OE3: Explicar el desarrollo alternativo de la investigación fiscal de la conducta delictiva de Vishing como nueva modalidad del delito informático en la Ley N° 30096 y su modificatoria Ley N° 30171 en el periodo 2020-2021				

CERTIFICADO DE VALIDEZ DE INSTRUMENTO

Instrucciones: Señor (a) especialista se le solicita su colaboración a fin de que posterior al análisis del presente instrumento, proceda a marcar con un aspa (X) según corresponda, de acuerdo a su criterio y experiencia profesional.

TÍTULO: LA REGULACIÓN DE LAS NUEVAS MODALIDADES DEL DELITO INFORMÁTICO EN LA LEY N° 30096 Y SU MODIFICATORIA, PERIODO 2020-2021										
N.°	CATEGORIAS	Pertinencia		Relevancia		Claridad		Suficiencia		Sugerencias
	AMBITO TEMÁTICO: LAS NUEVAS MODALIDADES DEL DELITO INFORMÁTICO	Si	No	Si	No	Si	No	Si	No	
1	¿Usted recibió charlas informativas, capacitaciones o cursos especializados en delitos informáticos, ofrecidas por el Ministerio Público u otra entidad? Precise.	X		X		X				
2	¿Durante el periodo 2020 al 2021 las denuncias en su despacho respecto a delitos informáticos incrementaron? De ser afirmativa su respuesta precise ¿Por qué?	X		X		X		X		
3	¿La falta de regulación específica de las nuevas modalidades del delito informático generan impunidad? ¿Por qué?	X		X		X				
4	¿Considera que las nuevas modalidades del delito informático deberían encontrarse reguladas en la Ley Nro. 30096, su modificatoria Ley N° 30171 o en el Código Penal? ¿Por qué?	X		X		X				

CATEGORIA 01: PHISHING		Pertinencia		Relevancia		Claridad		Suficiencia		Sugerencias
SUBCATEGORIAS: Web y correos electrónico, sujetos, conducta y bien jurídico protegido		Si	No	Si	No	Si	No	Si	No	
5	¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Phishing? De ser afirmativa su respuesta, especifique la cantidad.	X		X		X		X		
6	¿Cómo tipificó usted la conducta delictiva del Phishing?	X		X		X				
7	¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Phishing?	X		X		X				
8	¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Phishing? ¿Por qué?	X		X		X				
CATEGORÍA 02: SMISHING		Pertinencia		Relevancia		Claridad		Suficiencia		Sugerencias
SUBCATEGORIAS: SMS o mensajes, sujetos, conducta y bien jurídico protegido		Si	No	Si	No	Si	No	Si	No	
09	¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Smishing? De ser afirmativa su respuesta, especifique la cantidad.	X		X		X		X		

10	¿Cómo tipificó usted la conducta delictiva del Smishing?	X		X		X				
11	¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Smishing?	X		X		X		X		
12	¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Smishing? ¿Por qué?	X		X		X				
CATEGORÍA 03: VISHING		**Pertinencia**		**Relevancia**		**Claridad**		**Suficiencia**		**Sugerencias**
SUBCATEGORIAS: Voz o llamadas telefónicas, sujetos, conducta y bien jurídico protegido		**Si**	**No**	**Si**	**No**	**Si**	**No**	**Si**	**No**	
13	¿En su carrera fiscal se han presentado casos referentes a la conducta delictiva de Vishing? De ser afirmativa su respuesta, especifique la cantidad.	X		X		X				
14	¿Cómo tipificó usted la conducta delictiva del Vishing?	X		X		X		X		
15	¿Cuál es el estado procesal en el que se encuentran las carpetas fiscales referentes a la conducta delictiva del Vishing?	X		X		X				
16	¿Se debería incorporar un tipo penal específico para sancionar la conducta delictiva del Vishing? ¿Por qué?	X		X		X				

Observaciones: NINGUNA.

Opinión de aplicabilidad:

- Aplicable [X]
- Aplicable después de corregir [ ]
- No aplicable [ ]

DATOS DEL JUEZ EXPERTO VALIDADOR

Apellidos y nombres : TÚLLUME PISFIL VICTOR

DNI N° : 16627025

Profesión : ABOGADO - MAGISTER

Especialidad : DERECHO PENAL

Cargo : FISCAL PROVINCIAL TITULAR

Institución : MINISTERIO PÚBLICO

Huaraz, 27 de Setiembre del 2022.

Firma del experto

Anexo 04: Carta de consentimiento informado (participantes)

UNIVERSIDAD CÉSAR VALLEJO *FACULTAD DE DERECHO Y HUMANIDADES*

CARTA DE CONSENTIMIENTO INFORMADO

DIRIGIDO A : Fiscales de las Fiscalías Provinciales Penales Corporativas de Huaraz.

INSTITUCIÓN : Universidad César Vallejo – Sede Huaraz.

La presente investigación se denomina **"La Regulación de las Nuevas Modalidades del Delito Informático en la Ley N° 30096 y su Modificatoria, Periodo 2020-2021"**, la misma que es conducida por los estudiantes Ramos Caldua Mirian Caty y Salvador Rojas Yorman Andrey.

PROPÓSITO: La presente carta de consentimiento tiene el propósito de proveer a los participantes, una clara explicación de la naturaleza de la presente investigación, así como su rol de participante; asimismo, solicitarle su consentimiento informado para participar en él.

PROCEDIMIENTO: Si usted accede a participar en esta investigación, se le solicitara responder las preguntas a realizarse a través de una guía de entrevista, empleando un tiempo aproximado de 20 minutos, para su posterior transcripción y análisis a fin de fundamentar la regulación de las nuevas modalidades del Delito Informático en la Ley Nro. 30096 y su modificatoria, en el periodo 2020-2021. En ese sentido, su participación es estrictamente voluntaria puesto que la información que se recoja será confidencial ya su vez serán solo empleadas para fines académicos, no siendo usada para ningún otro propósito fuera de los de esta investigación.

RIESGOS: Usted no estará expuesto a ningún tipo de riesgo en la presente investigación.

BENEFICIOS: La presente investigación no conlleva beneficios directos para el participante, empero permitirá a los investigadores indagar aspectos referentes a las nuevas modalidades del Delito Informático en la Ley Nro. 30096 y su modificatoria, en el periodo 2020-2021.

Si tiene alguna duda sobre la investigación en mención, puede hacer preguntas en cualquier momento durante su participación en el. Igualmente, puede retirarse de la investigación en cualquier momento sin que ello lo perjudique en ninguna forma. Si alguna de las preguntas durante la entrevista le parece incómoda, tiene usted el derecho de hacérselo saber a los investigadores o de no responderlas.

COSTOS E INCENTIVOS: La participación en la investigación no tiene costo ni precio alguna, asimismo no recibirá algún incentivo económico ni de otra índole.

CONFIDENCIALIDAD: Garantizamos que los resultados e información que el participante provea en el curso de esta investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de esta investigación sin consentimiento del participante.

USO DE INFORMACIÓN OBTENIDA: Los resultados de la presente investigación serán conservados durante un periodo de 5 años de esta manera dichos datos pueden ser utilizados como antecedentes en futuras investigaciones relacionadas.

AUTORIZO A TENER MI INFORMACIÓN OBTENIDA Y QUE ESTA PUEDA SER ALMACENADA SI (X) NO ( )

DERECHOS DEL PARTICIPANTE: Si usted decide participar en la investigación, podrá retirarse de este en cualquier momento, o no participar en una parte de la investigación sin perjuicio alguno. De tener preguntas sobre su participación en esta investigación, puede contactar al correo de los investigadores: ysalvadorro@ucvvirtual.edu.pe o mramosca99@ucvvirtual.edu.pe, o en efecto a los siguientes números telefónicos: 931069880 – 947956819.

CONSENTIMIENTO: He escuchado la explicación de los investigadores y he leído el presente documento por lo que **ACEPTO** voluntariamente participar en esta investigación denominada **"La Regulación de las Nuevas Modalidades del Delito Informático en la Ley N° 30096 y su Modificatoria, Periodo 2020-2021"**, conducida por los estudiantes Ramos Caldua Mirian Caty y Salvador Rojas Yorman Andrey.

DATOS DEL PARTICIPANTE

NOMBRES : Renato Sulmer Arapa Diaz

PROFESIÓN O CARGO : Fiscal Provincial Penal

INSTITUCIÓN : Ministerio Público

FECHA Y HORA : 29 - 09 - 2022 17:10

Firma del Participante

RENATO SULMER ARAPA DIAZ
FISCAL PROVINCIAL TITULAR - COORDINADOR
3° FISCALÍA PROVINCIAL PENAL CORPORATIVA DE HUARAZ
MINISTERIO PÚBLICO
DISTRITO FISCAL DE ANCASH

CARTA DE CONSENTIMIENTO INFORMADO

DIRIGIDO A : Fiscales de las Fiscalías Provinciales Penales Corporativas de Huaraz.

INSTITUCIÓN : Universidad César Vallejo – Sede Huaraz.

La presente investigación se denomina **"La Regulación de las Nuevas Modalidades del Delito Informático en la Ley N° 30096 y su Modificatoria, Periodo 2020-2021"**, la misma que es conducida por los estudiantes Ramos Caldua Mirian Caty y Salvador Rojas Yorman Andrey.

PROPÓSITO: La presente carta de consentimiento tiene el propósito de proveer a los participantes, una clara explicación de la naturaleza de la presente investigación, así como su rol de participante; asimismo, solicitarle su consentimiento informado para participar en él.

PROCEDIMIENTO: Si usted accede a participar en esta investigación, se le solicitara responder las preguntas a realizarse a través de una guía de entrevista, empleando un tiempo aproximado de 20 minutos, para su posterior transcripción y análisis a fin de fundamentar la regulación de las nuevas modalidades del Delito Informático en la Ley Nro. 30096 y su modificatoria, en el periodo 2020-2021. En ese sentido, su participación es estrictamente voluntaria puesto que la información que se recoja será confidencial ya su vez serán solo empleadas para fines académicos, no siendo usada para ningún otro propósito fuera de los de esta investigación.

RIESGOS: Usted no estará expuesto a ningún tipo de riesgo en la presente investigación.

BENEFICIOS: La presente investigación no conlleva beneficios directos para el participante, empero permitirá a los investigadores indagar aspectos referentes a las nuevas modalidades del Delito Informático en la Ley Nro. 30096 y su modificatoria, en el periodo 2020-2021.

Si tiene alguna duda sobre la investigación en mención, puede hacer preguntas en cualquier momento durante su participación en el. Igualmente, puede retirarse de la investigación en cualquier momento sin que ello lo perjudique en ninguna forma. Si alguna de las preguntas durante la entrevista le parece incómoda, tiene usted el derecho de hacérselo saber a los investigadores o de no responderlas.

COSTOS E INCENTIVOS: La participación en la investigación no tiene costo ni precio alguna, asimismo no recibirá algún incentivo económico ni de otra índole.

CONFIDENCIALIDAD: Garantizamos que los resultados e información que el participante provea en el curso de esta investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de esta investigación sin consentimiento del participante.

USO DE INFORMACIÓN OBTENIDA: Los resultados de la presente investigación serán conservados durante un periodo de 5 años de esta manera dichos datos pueden ser utilizados como antecedentes en futuras investigaciones relacionadas.

AUTORIZO A TENER MI INFORMACIÓN OBTENIDA Y QUE ESTA PUEDA SER ALMACENADA SI (X) NO ( )

DERECHOS DEL PARTICIPANTE: Si usted decide participar en la investigación, podrá retirarse de este en cualquier momento, o no participar en una parte de la investigación sin perjuicio alguno. De tener preguntas sobre su participación en esta investigación, puede contactar al correo de los investigadores: ysalvadorro@ucvvirtual.edu.pe o mramosca99@ucvvirtual.edu.pe, o en efecto a los siguientes números telefónicos: 931069880 – 947956819.

CONSENTIMIENTO: He escuchado la explicación de los investigadores y he leído el presente documento por lo que **ACEPTO** voluntariamente participar en esta investigación denominada **"La Regulación de las Nuevas Modalidades del Delito Informático en la Ley N° 30096 y su Modificatoria, Periodo 2020-2021",** conducida por los estudiantes Ramos Caldua Mirian Caty y Salvador Rojas Yorman Andrey.

DATOS DEL PARTICIPANTE

NOMBRES : Ada del Rocio Quinajpe Asencio.
PROFESIÓN O CARGO : Abogada - fiscal.
INSTITUCIÓN : ministerio público
FECHA Y HORA : 06/10/2022 15:11.

Firma del Participante

CARTA DE CONSENTIMIENTO INFORMADO

DIRIGIDO A : Fiscales de las Fiscalías Provinciales Penales Corporativas de Huaraz.

INSTITUCIÓN : Universidad César Vallejo – Sede Huaraz.

La presente investigación se denomina **"La Regulación de las Nuevas Modalidades del Delito Informático en la Ley N° 30096 y su Modificatoria, Periodo 2020-2021"**, la misma que es conducida por los estudiantes Ramos Caldua Mirian Caty y Salvador Rojas Yorman Andrey.

PROPÓSITO: La presente carta de consentimiento tiene el propósito de proveer a los participantes, una clara explicación de la naturaleza de la presente investigación, así como su rol de participante; asimismo, solicitarle su consentimiento informado para participar en él.

PROCEDIMIENTO: Si usted accede a participar en esta investigación, se le solicitara responder las preguntas a realizarse a través de una guía de entrevista, empleando un tiempo aproximado de 20 minutos, para su posterior transcripción y análisis a fin de fundamentar la regulación de las nuevas modalidades del Delito Informático en la Ley Nro. 30096 y su modificatoria, en el periodo 2020-2021. En ese sentido, su participación es estrictamente voluntaria puesto que la información que se recoja será confidencial ya su vez serán solo empleadas para fines académicos, no siendo usada para ningún otro propósito fuera de los de esta investigación.

RIESGOS: Usted no estará expuesto a ningún tipo de riesgo en la presente investigación.

BENEFICIOS: La presente investigación no conlleva beneficios directos para el participante, empero permitirá a los investigadores indagar aspectos referentes a las nuevas modalidades del Delito Informático en la Ley Nro. 30096 y su modificatoria, en el periodo 2020-2021.

Si tiene alguna duda sobre la investigación en mención, puede hacer preguntas en cualquier momento durante su participación en el. Igualmente, puede retirarse de la investigación en cualquier momento sin que ello lo perjudique en ninguna forma. Si alguna de las preguntas durante la entrevista le parece incómoda, tiene usted el derecho de hacérselo saber a los investigadores o de no responderlas.

COSTOS E INCENTIVOS: La participación en la investigación no tiene costo ni precio alguna, asimismo no recibirá algún incentivo económico ni de otra índole.

CONFIDENCIALIDAD: Garantizamos que los resultados e información que el participante provea en el curso de esta investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de esta investigación sin consentimiento del participante.

USO DE INFORMACIÓN OBTENIDA: Los resultados de la presente investigación serán conservados durante un periodo de 5 años de esta manera dichos datos pueden ser utilizados como antecedentes en futuras investigaciones relacionadas.

AUTORIZO A TENER MI INFORMACIÓN OBTENIDA Y QUE ESTA PUEDA SER ALMACENADA SI (X) NO ( )

DERECHOS DEL PARTICIPANTE: Si usted decide participar en la investigación, podrá retirarse de este en cualquier momento, o no participar en una parte de la investigación sin perjuicio alguno. De tener preguntas sobre su participación en esta investigación, puede contactar al correo de los investigadores: ysalvadorro@ucvvirtual.edu.pe o mramosca99@ucvvirtual.edu.pe, o en efecto a los siguientes números telefónicos: 931069880 – 947956819.

CONSENTIMIENTO: He escuchado la explicación de los investigadores y he leído el presente documento por lo que **ACEPTO** voluntariamente participar en esta investigación denominada **"La Regulación de las Nuevas Modalidades del Delito Informático en la Ley N° 30096 y su Modificatoria, Periodo 2020-2021"**, conducida por los estudiantes Ramos Caldua Mirian Caty y Salvador Rojas Yorman Andrey.

DATOS DEL PARTICIPANTE

NOMBRES : Flor María Fernandez Castello
PROFESIÓN O CARGO : Fiscal Adjunta Provincial
INSTITUCIÓN : Ministerio Público
FECHA Y HORA : 06/10/2022

Firma del Participante

CARTA DE CONSENTIMIENTO INFORMADO

DIRIGIDO A : Fiscales de las Fiscalías Provinciales Penales Corporativas de Huaraz.

INSTITUCIÓN : Universidad César Vallejo – Sede Huaraz.

La presente investigación se denomina **"La Regulación de las Nuevas Modalidades del Delito Informático en la Ley N° 30096 y su Modificatoria, Periodo 2020-2021"**, la misma que es conducida por los estudiantes Ramos Caldua Mirian Caty y Salvador Rojas Yorman Andrey.

PROPÓSITO: La presente carta de consentimiento tiene el propósito de proveer a los participantes, una clara explicación de la naturaleza de la presente investigación, así como su rol de participante; asimismo, solicitarle su consentimiento informado para participar en él.

PROCEDIMIENTO: Si usted accede a participar en esta investigación, se le solicitara responder las preguntas a realizarse a través de una guía de entrevista, empleando un tiempo aproximado de 20 minutos, para su posterior transcripción y análisis a fin de fundamentar la regulación de las nuevas modalidades del Delito Informático en la Ley Nro. 30096 y su modificatoria, en el periodo 2020-2021. En ese sentido, su participación es estrictamente voluntaria puesto que la información que se recoja será confidencial ya su vez serán solo empleadas para fines académicos, no siendo usada para ningún otro propósito fuera de los de esta investigación.

RIESGOS: Usted no estará expuesto a ningún tipo de riesgo en la presente investigación.

BENEFICIOS: La presente investigación no conlleva beneficios directos para el participante, empero permitirá a los investigadores indagar aspectos referentes a las nuevas modalidades del Delito Informático en la Ley Nro. 30096 y su modificatoria, en el periodo 2020-2021.

Si tiene alguna duda sobre la investigación en mención, puede hacer preguntas en cualquier momento durante su participación en el. Igualmente, puede retirarse de la investigación en cualquier momento sin que ello lo perjudique en ninguna forma. Si alguna de las preguntas durante la entrevista le parece incómoda, tiene usted el derecho de hacérselo saber a los investigadores o de no responderlas.

COSTOS E INCENTIVOS: La participación en la investigación no tiene costo ni precio alguna, asimismo no recibirá algún incentivo económico ni de otra índole.

CONFIDENCIALIDAD: Garantizamos que los resultados e información que el participante provea en el curso de esta investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de esta investigación sin consentimiento del participante.

USO DE INFORMACIÓN OBTENIDA: Los resultados de la presente investigación serán conservados durante un periodo de 5 años de esta manera dichos datos pueden ser utilizados como antecedentes en futuras investigaciones relacionadas.

AUTORIZO A TENER MI INFORMACIÓN OBTENIDA Y QUE ESTA PUEDA SER ALMACENADA SI (X) NO ( )

DERECHOS DEL PARTICIPANTE: Si usted decide participar en la investigación, podrá retirarse de este en cualquier momento, o no participar en una parte de la investigación sin perjuicio alguno. De tener preguntas sobre su participación en esta investigación, puede contactar al correo de los investigadores: ysalvadorro@ucvvirtual.edu.pe o mramosca99@ucvvirtual.edu.pe, o en efecto a los siguientes números telefónicos: 931069880 – 947956819.

CONSENTIMIENTO: He escuchado la explicación de los investigadores y he leído el presente documento por lo que **ACEPTO** voluntariamente participar en esta investigación denominada **"La Regulación de las Nuevas Modalidades del Delito Informático en la Ley N° 30096 y su Modificatoria, Periodo 2020-2021",** conducida por los estudiantes Ramos Caldua Mirian Caty y Salvador Rojas Yorman Andrey.

DATOS DEL PARTICIPANTE

NOMBRES : Lizzeth Karen Avendaño Macedo
PROFESIÓN O CARGO : Fiscal Provincial Penal - Hz
INSTITUCIÓN : Ministerio Público - Ancash
FECHA Y HORA : 03/10/22, 16:48

Firma del Participante

CARTA DE CONSENTIMIENTO INFORMADO

DIRIGIDO A : Fiscales de las Fiscalías Provinciales Penales Corporativas de Huaraz.

INSTITUCIÓN : Universidad César Vallejo – Sede Huaraz.

La presente investigación se denomina **"La Regulación de las Nuevas Modalidades del Delito Informático en la Ley N° 30096 y su Modificatoria, Periodo 2020-2021"**, la misma que es conducida por los estudiantes Ramos Caldua Mirian Caty y Salvador Rojas Yorman Andrey.

PROPÓSITO: La presente carta de consentimiento tiene el propósito de proveer a los participantes, una clara explicación de la naturaleza de la presente investigación, así como su rol de participante; asimismo, solicitarle su consentimiento informado para participar en él.

PROCEDIMIENTO: Si usted accede a participar en esta investigación, se le solicitara responder las preguntas a realizarse a través de una guía de entrevista, empleando un tiempo aproximado de 20 minutos, para su posterior transcripción y análisis a fin de fundamentar la regulación de las nuevas modalidades del Delito Informático en la Ley Nro. 30096 y su modificatoria, en el periodo 2020-2021. En ese sentido, su participación es estrictamente voluntaria puesto que la información que se recoja será confidencial ya su vez serán solo empleadas para fines académicos, no siendo usada para ningún otro propósito fuera de los de esta investigación.

RIESGOS: Usted no estará expuesto a ningún tipo de riesgo en la presente investigación.

BENEFICIOS: La presente investigación no conlleva beneficios directos para el participante, empero permitirá a los investigadores indagar aspectos referentes a las nuevas modalidades del Delito Informático en la Ley Nro. 30096 y su modificatoria, en el periodo 2020-2021.

Si tiene alguna duda sobre la investigación en mención, puede hacer preguntas en cualquier momento durante su participación en el. Igualmente, puede retirarse de la investigación en cualquier momento sin que ello lo perjudique en ninguna forma. Si alguna de las preguntas durante la entrevista le parece incómoda, tiene usted el derecho de hacérselo saber a los investigadores o de no responderlas.

COSTOS E INCENTIVOS: La participación en la investigación no tiene costo ni precio alguna, asimismo no recibirá algún incentivo económico ni de otra índole.

07

CONFIDENCIALIDAD: Garantizamos que los resultados e información que el participante provea en el curso de esta investigación es estrictamente confidencial y no será usada para ningún otro propósito fuera de los de esta investigación sin consentimiento del participante.

USO DE INFORMACIÓN OBTENIDA: Los resultados de la presente investigación serán conservados durante un periodo de 5 años de esta manera dichos datos pueden ser utilizados como antecedentes en futuras investigaciones relacionadas.

AUTORIZO A TENER MI INFORMACIÓN OBTENIDA Y QUE ESTA PUEDA SER ALMACENADA SI (X) NO ( )

DERECHOS DEL PARTICIPANTE: Si usted decide participar en la investigación, podrá retirarse de este en cualquier momento, o no participar en una parte de la investigación sin perjuicio alguno. De tener preguntas sobre su participación en esta investigación, puede contactar al correo de los investigadores: ysalvadorro@ucvvirtual.edu.pe o mramosca99@ucvvirtual.edu.pe, o en efecto a los siguientes números telefónicos: 931069880 – 947956819.

CONSENTIMIENTO: He escuchado la explicación de los investigadores y he leído el presente documento por lo que **ACEPTO** voluntariamente participar en esta investigación denominada **"La Regulación de las Nuevas Modalidades del Delito Informático en la Ley N° 30096 y su Modificatoria, Periodo 2020-2021"**, conducida por los estudiantes Ramos Caldua Mirian Caty y Salvador Rojas Yorman Andrey.

DATOS DEL PARTICIPANTE

NOMBRES : Gurssela Zúñiga Rondán

PROFESIÓN O CARGO : Fiscal Adjunto Provincial.

INSTITUCIÓN : Ministerio Público

FECHA Y HORA : 04/10/22

Firma del Participante

UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Declaratoria de Autenticidad del Asesor

Yo, ORTEGA OBREGON DORIS LUZ, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - HUARAZ, asesor de Tesis titulada: "LA REGULACIÓN DE LAS NUEVAS MODALIDADES DEL DELITO INFORMÁTICO EN LA LEY N° 30096 Y SU MODIFICATORIA, PERIODO 2020-2021", cuyos autores son SALVADOR ROJAS YORMAN ANDREY, RAMOS CALDUA MIRIAN CATY, 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 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.

HUARAZ, 22 de Noviembre del 2022

Apellidos y Nombres del Asesor:	**Firma**
ORTEGA OBREGON DORIS LUZ **DNI:** 31609056 **ORCID:** 0000-0002-3264-2011	Firmado electrónicamente por: DORTEGAOB el 29-11-2022 08:32:18

Código documento Trilce: TRI - 0450382

INVESTIGA UCV