FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:

Abogada

AUTORAS:

Vigo Baca, Luz Benilda (ORCID: 0000-0003-1613-8568)

Zavala Alzamora, Karolein Mishel Magdelein (ORCID:0000-0003-2263-746X)

ASESOR:

Dr. Santisteban Llontop, Pedro Pablo (ORCID: 0000-0003-0998-0538)

LÌNEA DE INVESTIGACIÒN:

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

Lima – Perú

2021

Dedicatoria:

A mi familia por motivarme a estudiar constantemente, especialmente mis padres quienes me impulsa para lograr las metas trazadas y Caroline quien es mi estrella que siempre me guía - *Karolein Mishel Magdelein Zavala Alzamora.*

A mi mamá por su constante apoyo y acompañamiento en todo el trayecto de esta carrera, y a las personas que pusieron su confianza en mi y con sus motivaciones me permitieron a no rendirme – *Luz Benilda Vigo Baca*.

Agradecimientos:

Nuestra gratitud al docente Dr. Pedro Pablo Santisteban Llontop, quien compartió todos sus saberes, con esmero y dedicación. También agradecemos a los participantes de nuestra investigación, por su tiempo y contribución. Es preciso mencionar nuestra institución mater la Universidad César Vallejo que nos permitió formarnos como profesionales.

Índice de contenidos

Índice de tablas

Índice de gráficos y figuras

RESUMEN

La presente investigación titulada “Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020”, surgió de la necesidad de demostrar la problemática en que se encuentra el sistema peruano ante los delitos informáticos teniendo como consecuencia la afectación de los derechos patrimoniales. Tuvo como objetivo general Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Para ello, la investigación presenta un enfoque cualitativo, tipo básico, diseño de teoría fundamentada y nivel descriptivo; permitiendo recabar como hallazgo fichas de análisis documental, consolidadas con la aplicación de guías de entrevista a expertos de la materia; lo que ofreció a obtener como resultado y conclusión que , si se genera ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, dado que se comprende dentro de fraude informático todo los tipos de delito informáticos contra el patrimonio, el cual ocasiona un desmedro en la interpretación de la norma que no permite una sanción efectiva.

Palabras clave: Delito informático, ineficacia normativa, phishing.

ABSTRACT

This research entitled "Regulatory ineffectiveness for the protection of victims of phishing in financial entities, Lima 2020", arose from the need to demonstrate the problem in which the Peruvian system finds itself in the face of computer crimes, having as a consequence the affectation of rights patrimonial. Had as its general objective Analyze the effects generated by regulatory ineffectiveness for the protection of victims of phishing in financial entities, Lima 2020.

For this, the research presents a qualitative approach, basic type, the design of grounded theory and descriptive level; allowing to collect as a finding documents of documentary analysis, consolidated with the application of interview guides to experts in the field; what he offered to obtain as a result and conclusion that, if normative ineffectiveness is generated for the protection of victims of phishing in financial entities, given that all types of computer crime against patrimony are included within computer fraud, which causes a detriment in the interpretation of the norm that does not allow an effective sanction.

Keywords: Computer crime, normative ineffectiveness, patrimony.

I. INTRODUCCIÓN.- Referente a la **aproximación temática,** el informe de investigación tuvo mayor importancia debido a la evolución intelectual y científica de la humanidad que cada vez es más acelerada; ya que, la tecnología llegó a ocupar en nuestras vidas un lugar imprescindible en la rutina de las personas. Lo anteriormente descrito, se insertó en un proceso de globalización que conllevó a generar enormes cambios para la sociedad, en consecuencia, de los diversos delitos de la tecnología que infringieron a la estabilidad y protección a **nivel internacional**; tanto de las personas jurídicas como naturales. De esta manera, todos los países se unieron buscando pelear conjuntamente con la ciberdelincuencia, a través de un mejor sistema tecnológico de protección informática y legal; en este contexto, se consideró que la red general de ordenadores fue el cambio que compuso específicamente la realidad internacional y las interrelaciones de diversos sectores; donde se procesó la utilización de coordenadas entre un espacio y tiempo; transformándose en algo sustancial para nuestra vida, por ello debió ser tipificado correctamente ante estas crisis tecnológicas que venimos atravesando.

Junto a ello, la criminalidad no quedó al margen de tamaña influencia y se adaptó a nuevos aspectos, es ahí que la cibercriminalidad alude al grupo de acciones ilegales realizadas bajo el empleo abusivo de tecnologías, que se presentó bajo diferentes modalidades de sistemas o redes informáticas y generó una complejidad operativa y cambios constantes que dificultó su persecución. De este modo, uno de los sectores más vulnerados por esta tipología delictiva cibernética fueron las instituciones financieras y también la cadena de clientes víctimas de la ciberdelincuencia. El phishing evidenció lo señalado en estos casos; ya que, se utilizaron correos fraudulentos llevando a los usuarios desprevenidos a sitios web falsos para despojarlos de su dinero aparentando pertenecer a sitios web de entidades financieras, donde resaltó el abuso informático con la tentativa de obtener datos secretos de manera ilícita.

Es así, el desarrollo de la ciencia y la adhesión de una digitalización o variaciones de líneas, se vieron afectadas con más frecuencia por los accesos ilícitos a entidades financieras y a los consumidores a través del phishing o actividades con fines negativos para pasar como otro individuo; donde, el sujeto activo conocido como phisher, suplanta a un individuo o entidad financiera

simulando una intercomunicación de carácter oficial, también haciendo intercepciones telefónicas implicando que el sujeto activo envíe un correo electrónico al sujeto pasivo para que éste pueda “loguear” a la red. Logrando, que la víctima acceda a la página de internet creada para simulando confianza al usuario y éste presuma conocerla; pero, al verificarla esta “website” es sólo simulación, siendo el usuario víctima de phishing sin tener conocimiento de ello.

En consecuencia, respecto a la **formulación del problema**, se formuló en la investigación como **problema general**: ¿qué efectos genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020?; así mismo, el **problema específico 1** planteado fue, ¿cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa?, y el **problema específico 2** formulado fue, ¿cómo enfrentó el Ministerio Público la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras?.

Esas interrogantes se plantearon en base al resultado de las investigaciones estudiadas con relación al tema, considerando el contexto actual que resaltó escenarios de víctimas de phishing durante la pandemia, lo cual antes se habían suscitado, pero ahora es mayor la cantidad de estos actos ilícitos; trasluciendo la ineficacia normativa del art. 8 de la Ley N°30096 y las deficientes formulaciones de estos delitos en las comisarías y fiscalías.

Por consiguiente, se formuló la **justificación** de la investigación, partiendo de una **justificación teórica**, toda vez que la contribución del trabajo fue consecuencia del desarrollo conceptual de las categorías establecidas en la matriz realizada, estando la ineficacia normativa semejada con los vacíos legales, falta de valoración de la problemática social, desinstitucionalización; y la protección a las víctimas de phishing en entidades financieras como una manera de contrarrestar las deficiencias legales en este delito cibernético; lo cual, asociado a los resultados alcanzados por la ejecución de los instrumentos favoreció al empleo de la norma de una manera consecuente. En la **justificación práctica**, se evidenció que existen severos efectos a las víctimas de phishing en entidades financieras resaltando más en esta coyuntura social; en consecuencia, permitió hallar alternativas de solución que contribuirán a la asistencia en reuniones doctrinarias de especializaciones y

criterios normativos a considerarse para avalar el respeto hacia las decisiones emitidas influyendo en la baja de denuncias por esta modalidad, desplegando un razonamiento igual en la aplicación de la ley con la finalidad de una adecuada interpretación de leyes; ya que, los ciberdelitos se encuentra en la norma adjetiva penal en la Ley N°30096. Finalmente, respecto a la **justificación metodológica**, se empleó la entrevista y ficha de análisis de fuente documental para desempeñar el fin de la investigación, constituido en sus objetivos y siendo validados y revestidos de confiabilidad, inspirando a futuros proyectos de investigación. Es así, que se contribuyó formulando opiniones legales a considerarse con la intención de contrarrestar la ineficacia normativa de este delito.

Esto permitió formular el siguiente **objetivo general**: Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020; así como, entre sus **objetivos específicos** tenemos: i) Determinar como se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, ii) Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras.

De lo descrito anteriormente, se tuvo algunos supuestos que responden a cada cuestionamiento originado en la investigación; el **supuesto general** señala que la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima; generó como principales efectos, la falta de seguridad informática y daños patrimoniales; porque el usuario, consumidor o también denominado víctima, se encontró con discrepancias en el tratamiento de las leyes penales. Así también, el **supuesto específico 1** es**:** la protección a las víctimas de phishing en entidades financieras, fue vulnerado al no respetar el derecho de estas personas y por el mal actuar de los administradores de justicia; lo cual, se evidenció con las denuncias; y como **supuesto específico 2**: El Ministerio Público enfrentó la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras de una manera concreta y productiva; por ello, formó la Unidad Fiscal Especializada en Ciberdelincuencia, porque se observó el incremento de ciberdelitos en la modalidad phishing en la época de pandemia, sin embargo eso no fue suficiente.

II. **MARCO TEÓRICO.-** En relación a los **trabajos previos,** fue sumamente importante identificar y plasmar los **antecedentes** que provinieron de tesis y artículos de revistas indexadas sobre el procedimiento jurídico penal de los delitos informáticos en sentido amplio y en la modalidad de phishing, desarrollados con anterioridad a nivel nacional e internacional, empleados de complemento a los objetos propuestos en la investigación. En consecuencia, los **antecedentes del ámbito nacional**, se congregaron ciertas investigaciones que no solo plantearon a los delitos informáticos en sentido amplio, sino además refieren en particular sobre la modalidad de phishing y la ineficacia normativa en las víctimas de las entidades financieras. Se tuvo el gran aporte de la investigación de Pardo (2018), para la obtención de Maestro en Derecho Penal y Procesal Penal, por la Universidad César Vallejo, denominada: *"Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima , 2018"*, teniendo como objetivo general analizar el régimen jurídico penal de los delitos informáticos contra patrimonio, Distrito Judicial de Lima, 2018. La conclusión a la que se arribó fija a la regulación jurídica en el ámbito penal como inconsistente, todo ello partiendo de la afectación informática contra el patrimonio en diversas tipologías delictivas de ciberdelitos que generan inseguridad y miedo en la interpretación normativa, ya que no está tipificado la sanción estos delitos contra el patrimonio. En consecuencia, lo vertido por el autor se relacionó con el objetivo que se planteó en la investigación respecto al empleo legal en materia penal de delitos cibernéticos que es ineficaz, a pesar que en la legislación actual se sanciona este tipo de modalidad, no se reglamenta en forma clara y expresa la vulneración al patrimonio por medio de sistemas informáticos.

Asimismo, la investigación de Zorrilla (2018), para obtener el título de abogada, de la Universidad Nacional de Ancash "Santiago Antunez de Mayolo", denominada: *"Inconsistencias y ambigüedades en la Ley de delitos informáticos Ley N°30096 y su modificatoria Ley N°30171, que imposibilitan su eficaz cumplimiento"*, tiene el objetivo principal de determinar la intervención de la incongruencia y la oscuridad en la Ley Nº30096 y la Ley Nº30171 que la modifica; los cuales entorpecen su desempeño, teniendo una población de treinta licenciados en derecho, jueces y fiscales, donde se empleó como técnica de estudio la encuesta con el fin de poder conocer sus perspectivas acerca de las incongruencias y oscuridades de las leyes

señaladas, el tipo de estudio fue no experimental con diseño de corte trasversal, nivel de investigación es dogmático, empleando los datos recogidos con la encuesta. Concluyendo que existió una evidente imprecisión de acuerdo a la redacción por lo cual generó confusión e incertidumbre en relación a la Ley Nº30096 y la Ley Nº3017 que la modifica, donde se creó en muchas ocasiones desconciertos entre las partes procesales y limitó en cierta forma las formulaciones de denuncias o logró que el agente activo de este delito no se encuentre, imposibilitando que se sancionen a los verdaderos culpables. Además, la autora agregó que la falta de conocimientos informáticos agravó el crecimiento de estos delitos que se presentaron en nuestra realidad, desde este punto es necesario medidas preventivas de carácter penal más considerativas para este ilícito.

Podemos señalar, la investigación de Chilcon (2019), para obtener el título de doctor en desarrollo y seguridad estratégica, del Centro de Estudios Nacionales, titulada: *" El Cibercrimen en el Perú y su incidencia en la Seguridad Nacional"*, indicó el objetivo; determinar cómo la ciber delincuencia del Estado peruano perturba la Seguridad Nacional, el cual utilizó métodos de investigación en un enfoque cualitativo, y el diseño de estudio fue no experimental con una población de estudio que conciernen a directores y personal con capacitad de control en ciberdelicuencia, como instituciones de la PNP, MPFN y del PJ, que agrupan en total de 580 funcionarios y con una muestra de 231 sujetos, la técnica de recolección fue el cuestionario. De este modo, la conclusión que llegó el autor, señaló que la magnitud alcanzada por la ciberdelincuencia es significativa, siendo que afecta a la Seguridad Nacional, asimismo se planteó como recomendaciones crear estrategias para hacer frente a la ciberdelincuencia.

En la investigación creada por Espinoza (2017), para adquirir el título de abogado, por la Universidad Nacional del Altiplano, nombrada: *"Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control"*, tuvo como objetivo de estudio definir el DP informático , para el cual utilizó métodos de investigación como la dogmática jurídica, inductivo, deductivo, histórico, comparativo, analítico y sintético, señala que el DP informático tiene como finalidad el estudio de la seguridad jurídica y las leyes penales sobre delitos informáticos, cuyo propósito es reducir el poder de vigilancia del poder punitivo y se caracteriza

por ser represivo, público, fragmentador, contínuo y normativo; los delitos informáticos son transnacionales y multidisciplinarios. Este autor recomendó que se formulen propuestas legislativas de acuerdo a las reglas jurídicas generales en el ámbito internacional sobre el cuidado de comunicaciones y crear fiscalías especializadas en avances tecnológicos de información y de comunicación. Las conclusiones planteadas por el autor antes mencionado fueron bastantes relevantes y conllevaron a concordar en distintos puntos del objetivo específico 1 propuesto en la presente, puesto que reconoció la vulnerabilidad mediante las redes informáticas que acontecieron de imperfecciones regulatorias, conceptuales e informativas.

Finalmente, la investigacion desarrollada por Reyes (2020), para optar por el título de bachiller en derecho, por la Universidad Peruana de las Américas, denominada: *"Los delitos informáticos y su influencia en la integridad personal, distrito de Chorrillos, Lima Metropolitana, 2019"*, el objetivo general fue determinar la forma en que los delitos informáticos median en el derecho de todo individuo, es decir, la integridad. Se conformó una muestra empleando el cuestionario como instrumento, teniendo de técnica la encuesta y la metodología de estudio es enfoque cuantitativo. Se concluyó que la correlación conjunta entre los delitos informáticos y la integridad personal, es positiva o directa de 63.1% y un valor p=0,000 mediante el método de Spearman. De esta misma forma, el autor recomiendó que se logre realizar un trabajo conjunto con los operadores de justicia, además de capacitaciones constantes para el buen manejo y apoyo de las víctimas de diferentes variantes de delitos informáticos, con el fin de lograr la detección temprana, orientación y ejecución, los manejos de protocolos de seguridad de manera de que dichas personas puedan actuar diligentemente en sus acciones legales, policiales y penales correspondientes a su defensa de su integridad personal teniendo concordancia con el objetivo específico 2, ya que, consideró a los operadores de justicia y sus labores ineficaces que atentaron con el derecho de tutela.

Sobre los antecedentes averiguados en el **ámbito internacional**, el trabajo de investigación de Abdulai (2016), de la Universidad de Saskatchewan, que sustentó para optar el grado de Magister en Artes *"Determinantes del miedo a la victimización*

del crimen de cibernética: un estudio del fraude a la tarjeta de crédito / débito entre estudiantes de la Universidad de Saskatchewan" presentó como objetivo general investigar el miedo a la victimización por delito cibernético entre estudiantes de la Universidad de Saskatchewan. Entre sus conclusiones, destacó la experiencia de victimización y los comportamientos de uso de internet, los cuales, estuvieron coligados positivamente con el temor de los estudiantes y su riesgo a convertirse en víctimas de fraude con tarjetas de crédito/ débito. Lo planteado por este autor, supuso que es riesgosa la realización de transacciones por medios informáticos, en medida que exige revelación de datos secretos de la tarjeta, tal como lo plasmó en su problemática general que se encuentra a fines con el presente trabajo de investigación, porque se planteó que la identificación sociodemográfica de los estudiantes no estaba relacionada con su temor de victimización por fraudes con tarjetas de crédito/débito. Este abordaje concretizó el fin de poder revestir la normatividad de delitos informáticos, para preservar que no queden en la impunidad estos actos.

De la misma manera, es reveladora la investigación de Hidalgo (2018), para lograr el título de Abogado de los Tribunales y Juzgados de la República, por la Universidad Católica de Santiago de Guayaquil, llamada *"Los delitos informáticos y su afectación sobre los bienes jurídicos"*, presentando como objetivo general analizar el bien jurídico como la relación de un enfoque constitucional, social y su acaecimiento con los delitos informáticos. Entre sus conclusiones, se vislumbró que el crecimiento de la tecnología en base a los delitos cibernéticos, trata de mostrar las medidas y regulaciones en torno a los hechos que engloban la delicuencia informática, de tal motivo se debe enfatizar el estado actual de la ley penal nacional e internacional, con el propósito de que surga un equilibrio en la regulación de tipo penal. De este modo, el autor sugirió que es necesario transformar los enfoques y aspectos del procedimiento penal, siendo fundamental entender el ilícito criminal de delitos infomáticos como acciones de riesgo permitiendo un profundo estudio y cautela sobre los comportamientos de los agentes activos para la protección de la sociedad porque el tratamiento no cuenta con amparo efectivo y eficaz ante estos ilícitos. Cabe enfatizar, que tal referencia se encontró relacionado con la problemática general de la investigación, al mencionar la falta de tipificación de la criminalización de delitos informáticos con relación del bien jurídico protegido.

Por otra parte, la investigación realizada por Pons (2018), para obtener el título de doctorado en derecho y ciencias sociales, por la Universidad Nacional de Educación a Distancia, titulada *"Ciberterrorismo, amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional"*, presentando como objetivo general realizar un estudio de los aspectos subjetivos de este fenómeno criminal. La metodolgía de estudio en este trabajo de investigación fue el enfoque cualitativo y el diseño de estudio fue descriptivo y analítico, cuya población de estudio fue diez magistrados, veinte licenciados en derecho, ciento veinticinco encargados de la fuerza de seguridad de diferentes naciones, quienes se sometieron a una entrevista. Entre sus conclusiones resaltó que los países más evolucionados en tecnología, economía e infraestructura son los primeros en actuar, señalando que la forma efectiva de neutralizar el terrorismo cibernético es aumentando la seguridad del internet y estabilizando la legislación nacional, estas actuaciones permitirían reducir la impunidad e impedir diferencias en la prevención y persecución.

También, es valioso tomar en cuenta la investigación de Herrera (2016), para licenciarse como abogado, por la Universidad Central de Ecuador, que tiene como título: *"El Phishing como Delito Informático y su Falta de Tipificación en el Código Orgánico Integral Penal"*, presenta como objetivos determinar la deficiencia en la normativización de delitos informáticos de su legislación penal, que ocasiona impunidad. Entre sus conclusiones resaltó la idea que el tipo penal informático al no encontrarse establecido en la legislación penal incentiva la inseguridad e impunidad, por tales razones atenúa la falta de Protección legal de los afectados de esas acciones y es así que el órgano jurisdiccional no emplea la tutela judicial que todo individuo tiene derecho; olvidando el rol protector del estado sobre hacer valer las conjeturas para la protección de este delito, es claro la falta y necesidad de mecanismo para poder reconocer este tipo de ilícitos en el CP. Cabe precisar, que tal referencia se encontró relacionado con la problemática y objetivo general de la investigación, porque se hizo mención a la vulneración de las víctimas de phishing y evidenció los efectos de la carencia legal reflejados en la impunidad.

Prosiguiendo, en esta parte se expusieron los alcances conceptuales respecto de las categorías y sub categorías trazadas en la investigación, afines con la

ineficacia normativa para la protección de víctimas de phishing en entidades financieras partiendo de la relación con delitos informáticos. Por ello, es importante destacar las **teorías conceptuales;** donde se comprendió la supremacía de un marco teórico; en cuanto a la **primera categoría**, se presentó a la **ineficacia normativa** que correspondió a la inadecuación de la ley por parte de los miembros de diversas instituciones creadas para administrar justicia, porque la ley estipulada para esta materia no es precisa debido a la falta de capacitaciones; por eso, destacó la necesidad del empleo de rigurosidad y tipificación con las acciones en contra de las leyes informáticas establecidas, para que se efectúen consecuentemente al ámbito financiero; prevaleciendo el desafío del DP.

De ello, es transcendental desglosar la categorización esbozada, conformada por subcategoría 1 **marco legal,** donde se identificó todas las normativas establecidas en nuestro país para salvaguardar nuestros derechos como ciudadanos. En mención, a estas leyes tenemos Ley Nº30096, que permitió lidiar momentáneamente con el ciberdelito la cual fue modificada por Ley Nº30171, resaltando como bien jurídico al patrimonio, integridad, confidencialidad y disponibilidad de información. Se empleó simultáneamente el DL Nº635, modificado por el DL Nº1237, DL Nº1182 y Ley Nº28493; es importante, indicar que existe ineficacia ocasionada por la mala interpretación de la norma en base al phishing, toda vez que se evidenció casos archivados por la falta de calificación adecuada del delito, ausencia de acusación fiscal, carencia de individualización del autor.

Para conocer y comprender la subcategoría 2 **modalidades frecuentes en delitos informáticos,** se debe explicar qué es delito informático. Ahondando en el tema señalaremos los tipos que éste configura al ejecutar una acción delictiva, es decir, tipificada en el CP. En concordancia con ello, este tipo de modalidades se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica. Es así, que surgen las modalidades más conocidas: superzap, es una de ellas, comprende el sustento ideal, brindando acceso a programas para poder modificarlos sin que nadie se percate de ello; trampillas, es un portal oculto para ingresar a programas evadiendo las programaciones de vigilancia; vandalismo, son actos guiados por violencia para

eliminar o causar pérdidas en sistemas operativos de un sistema (virtual) y por último, hacemos mención a los virus de computadoras, estos infectan las composiciones de un sistema ocasionando daños de forma paulatina, obstruyendo el trabajo de una computadora o red.

Sobre la **segunda categoría** incumbió a las **víctimas de phishing**; definida como la población afectada por este ciberdelito direccionado a sistemas o redes informáticas, que mayormente son categorizados erróneamente con la figura de "estafas". En ese sentido, las subcategorías 1 **categorización de víctimas** y subcategorías 2 **actuación del Ministerio Público**, conducieron a la manifestación del Estado en este delito. El primero en mención, se refirió al sujeto pasivo de estos delitos cibernéticos quien puede ser persona natural o jurídica que es un ignorante en tecnología y por ello es más vulnerable; se clasifican en: Incursionistas, aquellos primerizos en la red que no se percatan de los virus que circulan y pueden verse afectados al acceder a un correo o sitio web; naturalistas, se consideran a los que atraviesan la juventud y ancianos, quienes creen que no existe la maldad o desean experimentar; discapacitados, quienes no pueden discernir rápidamente al sitio que están ingresando; exasperados, buscan algún sentimiento y por eso ingresan a cualquier grupo o red; aleatorios, son escogidos al azar. En la segunda subcategoría sabemos que todo operador de justicia debe manejar equipos actualizados; por ello, la actuación de la PNP y MPFN ante la modernización de la delincuencia; dicho esto, debemos evaluar nuestra realidad, es decir, la sobrecarga procesal, accesos tecnológicos, faltas de presupuestos; por el lado positivo sobresalió la creación de la única Fiscalía Especializada en Ciberdelincuencia en fecha dieciocho de setiembre del año dos mil veinte.

En consecuencia, se definió en los e**nfoques conceptuales** al término **phishing**, como el envío de diversos correos, con la intención que las víctimas no se percaten de la falsedad de estos y completen las informaciones requeridas, siendo una modalidad de delitos informáticos. Con respecto a la participación de las **entidades financieras** se mostró la falta de preocupación de estas empresas hacia sus usuarios, porque su único interés es ofrecer sus servicios financieros para intermediar y asesorar en el mercado de seguros o créditos, olvidando que ellos también se han visto perjudicados con esta modalidad de delitos informáticos.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

Este acápite sobre la línea de investigación, estableció la base o reglas del proyecto; por lo que, concernió trazar una adecuada metodología. Es así, que la característica principal de esta investigación fue que abarcó un **enfoque cualitativo**, de lo señalado por Hernández, Fernández y Baptista (2014), este asiste a un procedimiento no secuencial, lo cual significa que si bien las investigaciones de enfoque cuantitativo incorporan una específica exposición de cuestionamientos y formulación de hipótesis formuladas antes de la unión de todos los datos, los que desarrollen el enfoque cualitativo responderán las interrogantes y siendo esta nuestra metodología se expondrán los supuestos en el transcurso del acopio de todas las investigaciones.

Es precisa, la gran comparación entre los enfoques descritos porque no se relaciona solamente con el uso de métodos numéricos, todo lo contrario, se basa en la naturaleza de la investigación, que surgieron de la intención y enfoque que presentan considerando de esta manera que las investigaciones de enfoque cuantitativo contribuyen en una dirección externa u objetiva; pero, el enfoque cualitativo contiene un sentido inductivo que concierne una dirección interna o subjetiva como lo indica, Quintana (2006).

En consecuencia, el enfoque cualitativo presta atención a lo que pasa alrededor, basado en un entorno natural y en los sucesos; discriminando los fenómenos que acontecieron conforme a los hechos implicados.

Tipo de la investigación: Se ha tenido que es de tipo **básica**, relacionado al enfoque a seguir; por ello, Benito & Salinas (2016) menciona, que está conformado como lo encamina su nomenclatura en las bases de diversas investigaciones y principalmente se emplea en ciencias abstractas. Asimismo, Valderrama (2015) concuerda que la investigación básica o llamada también pura posee una característica teórica, la cual no está diseñada para solucionar problemáticas puramente prácticas.

Por otro lado, es de necesidad mencionar que, el presente trabajo buscó aumentar el conocimiento teórico, empleándose conforme al nivel de

investigación **descriptiva**, que permitió a la presente manifestar la problemática diseñada; según, Morales (2012) gran parte de investigaciones ejecutan este nivel porque delimita un fenómeno sobre las características vinculadas en los rasgos propios. En consecuencia, se averiguó para describir el problema planteado y de la población utilizada se examinó los resultados que permitieron trazar una idea y crearla como teoría.

Por esa razón, no se manejó la información reunida de las fuentes empleadas, ni la problemática que se estudió; porque se orientó en la exploración de describir el objetivo de la investigación, sin ninguna alteración.

Diseño de investigación: Al existir, varias clases de diseños generales de investigación, considerando el poder del investigador hacia las variables observamos diseños experimentales o no experimentales y asemejándolo al tiempo se encuentran los diseños seccionales y longitudinales. Es así, que la investigación utilizó la **Teoría Fundamentada**, que busca representar adecuadamente una teoría que se guiará de experiencias para la base datos y el desarrollo corresponde a ciencias sociales, al cual pertenece el Derecho, como lo manifiestan Hernández, Fernández, & Baptista (2014).

Entonces, a través de la teoría fundamentada se encontró de forma amplia la problemática de estudio, de este modo, se contribuyó con nuevas visiones con el empleo de la interpretación. Lo cual, logró la formulación de una teoría nueva generada del proceso y análisis de la recolección de datos, además las contribuciones del derecho examinados en la parte teórica también ayudaron a la formulación de teorías que respondieron a los objetivos trazados.

3.2. Categorías, Subcategorías y matriz de categorización:

Las interrogantes de la presente investigación estuvieron desarrolladas en dos categorías (Ineficacia Normativa y Víctimas de Phishing) donde la finalidad fue encontrar la relación entre ambas, es decir, describir los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020. En consecuencia, se solicitará la modificación legal de los ciberdelitos de acuerdo a sus modalidades, basados en una proposición teórica que explique el problema de investigación y otorgue soluciones.

Aquellas conclusiones estuvieron planteadas conforme a las teorías conexas a nuestra temática, de acuerdo a los datos e información acumulada en el desarrollo de la investigación.

Es necesario, indicar que la categoría inmersa en el enfoque cualitativo, formó la idea central que se dirigió la investigación, creando una definición precisa que no varía su contexto así este unida a otra. De ello, se desprende que las subcategorías contribuyeron al deslinde conceptual, clasificaciones, que se investigaron, teniendo como función principal coadyuvar al problema general y problemas específicos.

En consecuencia, la **primera categoría** fue; Ineficacia Normativa que atañe a la inaplicación legal por las autoridades judiciales, porque la legislación de esta materia no es clara; de ello se desprendió la **subcategoría 1**, marco legal y **subcategoría 2** modalidades frecuentes en delitos informáticos.

El marco legal, abarca las leyes estipuladas por nuestros juristas, el cual se basa en el iusnaturalismo y positivismo para garantizar la presencia del estado ante los problemas sociales, puesto que principalmente toda actividad delictiva merece una sanción y por ello debe estar contenido en el marco normativo, ya que representa un riesgo o amenaza a la seguridad teniendo en cuenta que para ser catalogado delito debe estar contenido en la ley penal; asimismo, debemos tener en cuenta que recién en el año dos mil diecinueve nuestro país formó parte del Convenio contra la Ciberdelincuencia conocido como Convenio de Budapest, en el cual figuran las estipulaciones legales. Además, el bien jurídico protegido en la normatividad se fundamenta principalmente en la información difundida por datos y también en el bien dañado como en phishing.

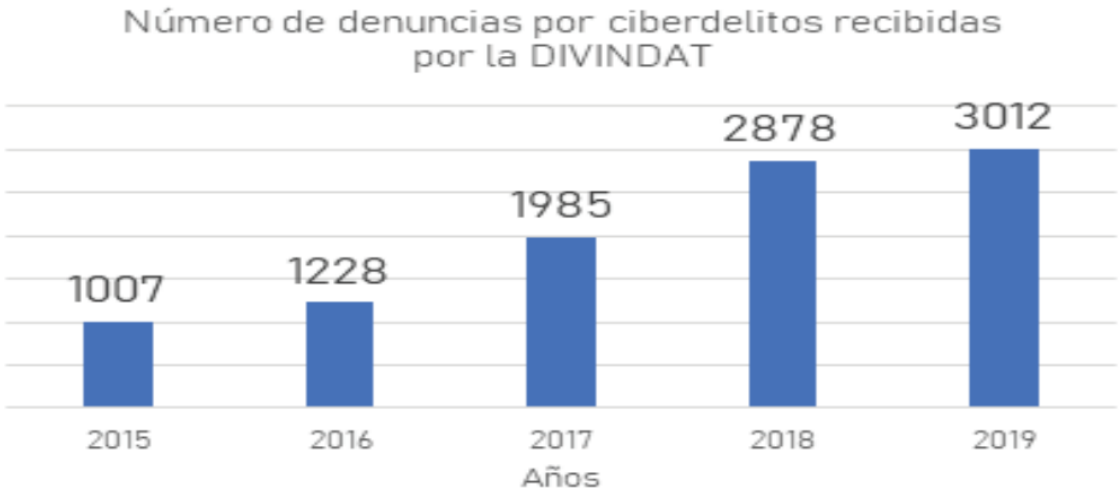
El segundo, modalidades frecuentes en delitos informáticos, se refiere a las características que puede adoptar este delito; puesto que, con el transcurrir de los años los avances tecnológicos han sido un mecanismo para vulnerar medios informáticos dañando a terceros, resaltando el phisphing con un alto nivel de incidencia; donde se ejecuta con el envío de un correo y mandan un enlace, por ejemplo haciéndose pasar por un banco donde posteriormente robarían los credenciales y sustraerían el dinero. Sin embargo, se debe explicar la definición de informática que es un grupo de informaciones lógicas y computarizadas que permite llegar a puntos de vistas coherentes y eficaces;

partiendo de ello, Rodríguez (2013), explica que el conjunto de reglas normativas sobre informática son el procedimiento para regular en éste ámbito legal referente a todas sus manifestaciones de aplicaciones.

En consecuencia, se relacionó los delitos informáticos con el phishing, explayándose en el tema Leukfeldt, E. (2014) quien comprobó que los conjuntos de personas envueltas en phishing son de diversas características que podrían cambiar el modus de actuar ante estos delitos, ya sea por su entorno social, lugar de formación, que se relaciona con el gran portal en las redes incluso observando otras conveniencias delincuenciales.

Sobre la **segunda categoría** de víctimas de phishing; hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, que mayormente no son categorizados con el tipo penal adecuado, porque se confunde con la figura de “estafas”. Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019), señala en su estudio la manera de concientizar y enseñar a las personas para que no sean víctimas de phishing y a la vez eviten mostrar informaciones en la red, teniendo como una forma de educación de estos delitos al “Phish1 game”, un juego que ayuda a infundir a la sociedad sobre los riesgos del phishing. A fin de, reflexionar debido a los altos índices de denuncias que van constantemente en crecimiento en nuestro país, se muestra la siguiente figura.

Figura 1. Tipología General de Violencia



Fuente: Estadística DIVINDAT – DIRINCRI PNP / Elaboración: Observatorio INDAGA

La figura, indica las cifras de afirmaciones formales sobre unas conductas informáticas sancionadas por la ley (ciberdelitos) que competen a la DIVINDAT, demostrando la cantidad de Víctimas que aumentan cada año y la considerable diferencia de estos casos entre los años anteriores con el 2019; por ese motivo, se considera alarmante el grado de complejidad y la ineficiente actuación de las autoridades que administran la justicia sobre este tipo penal, materia de la investigación.

De ahí, se desprende los hechos materia de formalización de denuncias ante el MPFN, que en el año 2020 se han venido ejecutando en los casos de ciberdelitos; por eso se enseña la *figura 2*, donde se aprecia el rol que han tratado de cumplir los agentes de justicia con la intención de mitigar este delito en algunos distritos fiscales, como Lima que está primero en la incidencia de estos.

Figura 2. Casos de ciberdelitos contra el patrimonio atendidos por el MPFN

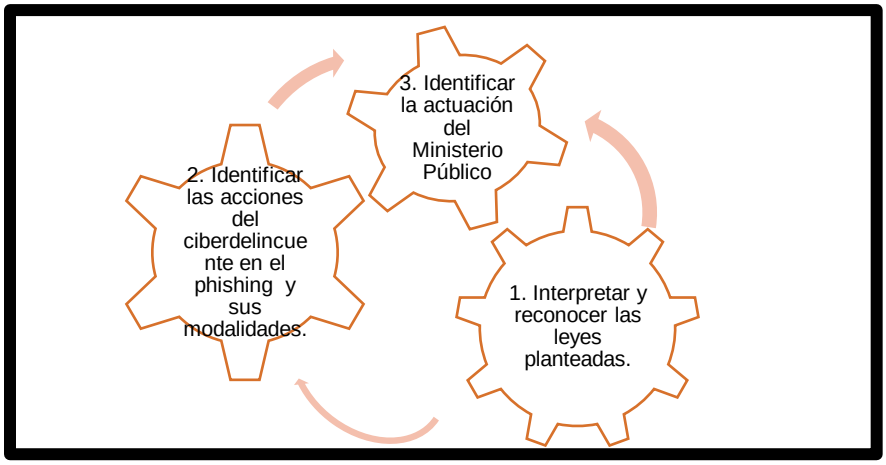
Distrito fiscal	Casos	%
Lima	405	22.7%
Lima Este	326	18.2%
Lima Norte	272	15.2%
Arequipa	177	9.9%
Callao	102	5.7%
Ica	88	4.9%
Lima Sur	64	3.6%
Otros	354	19.8%
Total	1,788	100%

Fuente: SIATF – SGF, Ministerio Público

En ese sentido, la **subcategoría 1** categorización de víctimas y **subcategoría 2** actuación del MPFN, conducen a la manifestación del Estado en este delito; el primero, supone el perfil de las Víctimas conectada a los ciberdelincuentes, considerados como los autores identificados; el segundo, muestra las formas de contrarrestar el Phishing a través del MPFN, involucrando las nuevas directrices a seguir en cuanto la normatividad, que evidentemente no ha funcionado a pesar de la creación de la Fiscalía

Especializada en Ciberdelincuencia, que no concuerdan con la PNP para por lo menos hacer una tipificación adecuada del delito en mención que ha venido afectando gravemente a las víctimas de este.

Figura 3. Mecanismos para reconocer la acción penal en la investigación



La Figura 3, tiene como propósito la indicación de las pautas con el fin de conocer las etapas realizadas para este trabajo, sobre el cumplimento de los mecanismos para reconocer la acción penal en la investigación.

Es necesario señalar, que, en la **matriz de categorización apriorística**, se estableció de forma completa, detalles claros y precisos con los lineamientos establecidos para el desarrollo de esta investigación y así se pudiera llegar a concretar; conteniendo los siguientes datos: título de la investigación, problema general, problemas específicos, objetivo general, objetivos específicos, categorías y subcategorías, explicadas en los acápites anteriores.

De lo expuesto, se percibió conveniente sintetizar cada categoría y subcategorías en la siguiente tabla:

Tabla N° 01. Tabla de categorías y subcategorías

Categorías	**Subcategorías**
1.Ineficacia normativa	1.Marco legal.
	2.Modalidades frecuentes en delitos informáticos.
2.Víctimas de phishing	1.Categorización de víctimas.
	2.Actuación del Ministerio Público.

3.3. Escenario de estudio:

Es el lugar o espacio territorial en el cual, se recolectó los datos, aplicando los instrumentos que luego se establecieron y validaron siendo comprendido por el ambiente físico. Por ello, el escenario fue en Lima, donde la aplicación de la entrevista como una de las bases de la investigación se realizó a los abogados especialistas en materia penal y policías que manejan un deslinde conceptual amplio del problema de esta investigación, persiguiendo la comisión de presuntos delitos y guiando el proceso penal, siendo el entorno primordial, el ambiente de trabajo donde realizan sus labores, es decir, la Fiscalía Especializada en Ciberdelincuencia, DIVINDAT y abogados litigantes especialistas en derecho penal; que forman parte del MPFN, PNP y despachos legales, respectivamente.

3.4. **Participantes**:

Sobre la muestra, fue no probabilística porque se consideró las características de la investigación sobre los elementos que estuvieron relacionados con aportar a los propósitos trazados, es así, que no se basa en fórmulas determinadas, pues siguió las decisiones tomadas durante la investigación; respetando los lineamientos y escogiendo la muestra orientada con el planteamiento del problema, diseño de la investigación y aportes conseguidos.

En este punto, se detallará la categorización de sujetos, que indica a aquellas personas que serán materia de aplicación del primer instrumento, la entrevista, los cuales serán llamados **participantes**, quienes son abogados especialistas en la materia penal, desde fiscales hasta abogados litigantes, en la presente se contará con dos Fiscales Especializados en Ciberdelincuencia, dos abogados litigantes y dos policías de la DIVINDAT, lo cual detallamos a continuación:

Tabla N° 02. Tabla de escenario de estudio y participantes

ESCENARIO DE ESTUDIO	PARTICIPANTES
Primer Juzgado de Investigación Preparatoria de Villa María del Triunfo	Juez Lenin Aldo Segundo Ayala

12° Juzgado Penal Unipersonal de la Corte Superior de Justicia de Lima Norte	Juez Luis Alberto Alvarez Torres
Fiscalía Adjunta Provincial Penal de Los Olivos- Lima Norte	Fiscal Jose Luis Borda Rubatto
Ministerio del Interior	Ex Director de delitos contra el crimen organizado – Magister Salvattore Leonardo Tripi Rossel
Asesor 2 del congresista César Manuel Revilla Villanueva – Partido Político Fuerza Popular	Victor Eduardo Augusto Moran Leon
División de investigación de delitos de alta tecnología (DIVINDAT) de la Policía Nacional del Perú	Ex jefe de equipo de investigaciones – Comandante Juan Antonio Pozo Castillo
División de investigación de delitos de alta tecnología (DIVINDAT) de la Policía Nacional del Perú	Analista informático forense - Ingeniero Wuilman Zabarburu Vargas
Fiscalía Adjunta Provincial Penal de Distrito Fiscal del Callao	Ex fiscal - Del Rio Espinoza Jorge Fernando
Estudio Jurídico	Nino Alvarez Torres
Estudio Jurídico	Doctor Gustavo Vilchez Cordero
Estudio Jurídico	Juan Jose Paredes Cordero
TOTAL	**11** participantes

3.5. Técnicas e instrumentos de recolección de datos:

El propósito de recolectar datos que fueron utilizados en este trabajo de investigación, proviene de Hernandez, Fernández, & Baptista (2014) quienes manifiestan, la explicación de los instrumentos y método empleado; además, es importante enfatizar que la recolección es esencial al igual que la información alcanzada que servirá como fuente de análisis para dar respuesta a la problemática planteada. Teniendo en cuenta lo señalado, en este trabajo se aprovechará la técnica de entrevista y análisis de fuente documental

alcanzando como instrumentos la entrevista y la ficha de fuente de análisis documental.

La técnica de entrevista es todo lo opuesto a una encuesta, puntualizando que la segunda en mención pertenece al enfoque cuantitativo y deja interrogantes; la entrevista tiene carácter trascendental porque la información captada sobre las respuestas del entrevistado permite avanzar sobre el fondo de la investigación .En conclusión, esta técnica logrará que la información surgida de los objetivos trazados permitan responder las interrogantes desde el punto de vista de profesionales especializados adecuadamente identificados.

En consiguiente, se empleó la **entrevista**, la cual es la manera de expresar como instrumento de la técnica de entrevista, a través de interrogantes expuestas que serán resueltas por los colaboradores mencionados en los acápites anteriores. Es así, que las preguntas contendrán objetividad, serán concretas, abiertas y asimilables al entrevistado; por ello, se redactarán nueve preguntas, tres de ellas esgrimidas del objetivo específico, tres referentes al objetivo específico 1 y tres para el objetivo específico 2; teniendo en cuenta que todo lo redactado se efectuará en base al marco teórico, específicamente esto concierne a los trabajos previos, categorías y subcategorías.

Asimismo, se utilizó la **técnica de análisis de fuente documental** definida como método creado para individualizar cada documento y lo que éste representa; permitiendo encontrar el documento principal a través de otro que se denominaría como secundario, manteniendo un orden para las búsquedas posteriores o salvación de informaciones.

La ficha de fuente de análisis documental, está personificada por la forma de expresar la técnica antes señalada, siendo el instrumento en sí, empleando la observación e interpretación de legislación nacional e internacional relacionadas a las categorías de esta investigación, perteneciendo a materia penal, procesal penal y legislación comparada sobre las normas empleadas para contrarrestar el Phishing en otros países.

Los instrumentos que se utilizaron en relación a la técnica de análisis de fuente documental, fueron las fichas de fuente de análisis documental:

Jurisprudencia internacional, derecho comparado, informe de análisis, artículo informativo en página web, resolución de la Fiscalía de la Nación; todas las mencionadas fueron realizadas a través de fichas de análisis de fuentes documentales que ayudaron en el análisis de la investigación. Siendo empleadas en relación con las muestras tomadas de los participantes especialistas en el tema abordado; de ello se desprende, que las preguntas y respuestas se encontraban encaminadas para responder al objetivo de la investigación. De igual manera, las fuentes de información suscritas, aportaron datos importantes para defender las teorías formuladas; teniendo en cuenta la validez en señal de aprobación.

Después de lo manifestado, se esquematizó la validación mencionando el porcentaje establecido de la guía de entrevista, considerando los docentes el porcentaje del 95%, que se mostrará a continuación:

Tabla N° 03. Tabla de validación de la guía de entrevista

VALIDACIÓN DE INSTRUMENTOS – GUÍA DE ENTREVISTA		
DOCENTES	**CARGO**	**PORCENTAJE**
Dr. Pedro Pablo Santisteban Llontop	Docentes de metodología de investigación científica en la Universidad César Vallejo	95%
Mg. Eliseo Segundo Wenzel Miranda		95%
Luca Aceto		95%
	PROMEDIO	95%

3.6. Procedimientos:

La formulación agrupada de los métodos para obtener datos, englobó la fabricación entre planificar con la finalidad de unir y ordenar todas las informaciones conseguidas sobre las categorías de ineficacia normativa y víctimas de phishing; para luego elaborar las conclusiones que conciban de confianza y seguridad a todos los resultados emanados de ellas.

Entonces, se recogerán los datos, se convertirán y comprobarán para tener respuesta a los objetivos trazados; considerando la siguiente tabla de categorías, subcategorías y de cada objetivo derivado del trabajo de investigación, los cuales se mostrarán en las siguientes tablas:

Tabla N° 04. Tabla de libros empleados para categorías y subcategorías

CATEGORÍA 1: Ineficacia normativa				
Subcategoría	**Nombre del libro**	**Autor**	**Año**	**País**
1.Marco legal	Ley de delitos informáticos Ley N°30096	Promulgada en gobierno de Ollanta Humala Tasso - Presidente Constitucional de la República.	2014	Perú
2.Modalidades frecuentes	Manual de Derecho Penal Informático	Juan Carlos Jimenez Herrera	2017	Perú
CATEGORÍA 2: Víctimas de phishing				
Subcategoría	**Nombre del libro**	**Autor**	**Año**	**País**
3.Categorización de víctimas	El bien jurídico protegido en el delito de estafa	Javier Sanchez Bernal	2009	España
4.Actuación del Ministerio Público	-Responsabilidad Penal de los muleros del Phishing. -Ciberdelincuencia en el Perú: Pautas para una investigación fiscal especializada.	-Elena Beatriz Fernández Castejón. - Oficina de análisis estratégico contra la criminalidad.	2015 2021	España Perú

Tabla N° 05. Tabla de tesis empleado para el objetivo general

OBJETIVO GENERAL: Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.				
Categoría	**Nombre de la tesis**	**Autor**	**Año**	**País**
Tesis de Grado	Los delitos informáticos y su afectación sobre los bienes jurídicos.	-Jorge Adrian Hidalgo.	2018	Ecuador
Tesis de Grado	El Phishing como Delito Informático y su Falta de Tipificación en el Código Orgánico Integral Penal.	-Edwin Ángel Herrera Calderón.	2016	Ecuador
Tesis de Grado	Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016.	-Diego Alexander Alarcon Ariza. -Javier Antonio Barrera Barón.	2017	Perú
Tesis de Grado	Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018.	-Alejo Pardo Vargas.	2018	Perú
Tesis de Maestría	Determinantes de miedo a la victimización del crimen de cibernética: un estudio del fraude a la tarjeta de crédito/ débito entre estudiantes de la Universidad de Saskatchewan.	-Abdulai Mohammed.	2016	Canada

Tabla N° 06. Tabla de tesis empleado para el objetivo específico 1

OBJETIVO ESPECÍFICO 1: Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa.				
Categoría	**Nombre de la tesis**	**Autor**	**Año**	**País**
Tesis de Grado	El cibercrimen en el Perú y su incidencia en la seguridad nacional	Miriam Chilcon Silva	2019	Perú
Tesis de Grado	Adopción de estrategias de ciberseguridad en la protección de la información en la oficina de economía del ejército , San Borja-2017.	John Justo Sanchez Blas	2017	Perú
Tesis de Grado	Inconsistencias y ambigüedades en la Ley N°30171, que imposibilitan su eficaz cumplimiento.	Karina Joselin Zorrilla Tocto	2018	Perú

Tabla N° 07. Tabla de tesis empleado para el objetivo específico 2

OBJETIVO ESPECÍFICO 2: Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras.				
Categoría	**Nombre de la tesis**	**Autor**	**Año**	**País**
Tesis de Grado	Los delitos informáticos y su influencia en Integridad Personal, distrito de Chorrillos, Lima Metropolitana, 2019.	Carlos Alberto Reyes Valdivia	2020	Perú
Tesis de Grado	Derecho Penal Informático: Deslegitimación del poder punitivo en la sociedad de control.	Michael Espinoza Coila	2017	Perú
Tesis Doctoral	Ciberterrorismo: Amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional.	Vicente Pons Gamon	2018	España

3.7. Rigor científico:

Para Erazo (2011), señala que cuando se hace referencia a rigor científico, debemos asemejarlo con la veracidad y estructura social impuesta en cada parte que se alcanzará en el presente trabajo.

De ello se desprende, que este acápite se basa en la reunión de todos los datos y la averiguación obtenida según los lineamientos científicos establecidos; los cuales se construyen teóricamente con las categorías y subcategorías vinculadas a una debida exegesis. Teniendo en claro lo mencionado, debemos resaltar que el presente trabajo está formulado con rigor científico, demostrado con la validación de todos los instrumentos esgrimidos.

3.8. Método de análisis de la Información:

El conjunto de métodos empleados, serán parte de la interpretación de los resultados logrados, elaborados y explorados exhaustivamente, buscando el producto final concreto y sintetizado ceñido a la teoría fundamentada; conformada por **hermenéutico**, porque enunciará la interpretación y opinión de los participantes para contribuir al trabajo; **inductivo**, porque sobre las explicaciones de los especialistas se deducirá las conclusiones y **descriptivo**, toda vez, que lo recaudado de las informaciones hace referencias a características y cualidades de lo que pasa en un momento determinado.

3.9. Aspectos éticos:

Definitivamente en este párrafo, se caracteriza el valor del respeto a la norma jurídica, ética, moral y social establecidas de las fuentes del derecho; en consecuencia, no se transgrede de ninguna manera el derecho de las partes relacionadas. Por ello, la recolección de datos, será empleado con la aprobación de los entrevistados, comprometiéndonos a la reserva y seguridad que amerite la presente investigación. Es de vital importancia, manifestar que las fuentes empleadas en el transcurso de la investigación serán citadas bajo el modelo estándar del conjunto de normas, acatando los derechos de autor.

IV. RESULTADOS Y DISCUSIÓN

En este apartado, se mostrará e dilucidará las informaciones recabadas de los instrumentos de recolección elaborados; posterior a ello, se someterá a discusión y crítica con el empleo de métodos de análisis detallados anteriormente. Consideraremos la ausencia de los lineamientos o modelos para el reporte de resultados y el desarrollo de la discusión, para de este modo concretar con autonomía la forma, teniendo en cuenta el contenido, importancia y fondo de la exposición y discusión que repercutió de las acciones realizadas para obtener las fuentes.

A pesar del respectivo comienzo, que debemos considerar, se dispuso una estructura en base a los métodos de procesos de conocimientos que permita entender al público lector y a la comunidad académica las conclusiones que este trabajo arribará. Entonces, nos comprometemos a establecer la presentación de los resultados en función del orden seguido en la exposición de los objetivos: iniciando por el objetivo general y posteriormente los dos objetivos específicos.

Debido a que, las fuentes empleadas nacen de la información recabada de los expertos y documentos, los resultados de cada una de ellas se expondrán por separado; iniciando por las respuestas de los especialistas conocedores quienes fueron entrevistados, agrupándose por cada pregunta formulada en la entrevista, después, se consignarán los hallazgos de las fuentes documentales. Es preciso manifestar, que la severidad en el intercambio de información de los resultados y en la discusión no descarta el aporte único que ofrece el investigador; ya que, se debe recordar que se emplea el enfoque cualitativo y el diseño de teoría fundamentada.

Definitivamente, se obtendrán los resultados basados en la razón individual, considerando que son insumos apoyados de la perspectiva teórica relacionada con las conclusiones; dicho esto, observaremos que en esta investigación el contenido de los resultados no establece el fundamento de las conclusiones. A partir de ello, teniendo claridad de la investigación realizada, se da inicio al informe de resultados.

Del **objetivo general** “Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020”.

Respuestas de los expertos entrevistados.

Cuando a los expertos se les formuló la interrogación, **¿de qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?**.

Segundo (2021) indicó, la ineficacia normativa resalta al no haber una legislación que proteja a la victima del phishing , pues las entidades bancarias e INDECOPI, determinan responsabilidad en el cliente.Además, existe una disyuntiva si el phishing es un delito informático o una estafa por que el fin es el hurto del dinero que se encuentra en la cuenta de ahorros o en la tarjeta de crédito,sin tomar en cuenta el medio por el cual realiza dicha acción.

Alvarez (2021), dice que la insuficiente tipificación del delito en el ámbito informático y su insuficiente control a nivel de la legislación genera desprotección a las víctimas de phishing.

Borda (2021) señala, que dado el estado de emergencia que la nación ha sufrido que los ciudadanos realicen y efectúen un mayor uso de la tecnología para la adquisición de bienes y servicios, muchas veces de ellos las entidades prestadoras de estos servicios solicitaban que las transferencias se efectuaran mediante las modalidades en línea, por ejemplo la compra de víveres de Wong, mi banda y etc., entonces se ha realizado, empero muchas veces ha pasado que las páginas web fueron clonadas, con el fin de vulnerar el servicio y la legislación tiene un vacío, dado que existe una afectación al consumidor, lo cual ha procedido con las denuncias de fraude informático y las entidades financieras y de servicios no han podido solucionar esta situación, puesto que no existe legislación alguna que en cierta medida haya podido resolver este conflicto de intereses.

Tripi (2021) resalta, no es la ineficacia de las normas las que generan un problema en la protección de los usuarios y/o clientes de las entidades bancarias, son los niveles de seguridad de los procesos en entidades bancarias que tienen problemas para la protección en contra de los casos de cibercrimen.

Pozo (2021) menciona, el phishing como modalidad delictiva no está tipificada en la Ley de Delitos Informáticos Nº 30096 se comete a través del internet mediante el uso de ingeniería social, es un virus que es enviado por los ciberdelincuentes en forma masiva con una con una página falsa de una entidad bancaria donde generalmente indican que actualice sus datos o se ha hecho acreedor a una promoción al hacer clic en este vínculo lo re direcciona a otra página falsa del banco y le capta los datos confidenciales de su tarjeta electrónicas bancarias, ahora bien la entidad bancaria es la responsable que su cliente haya ingresado sus datos confidenciales en una página falsa y le hayan captado estos datos para posteriormente ser usados en forma inmediata por realizar transferencias ilícitas de dinero o realizar compras por internet, en este caso el cliente es el responsable ya que no tiene instalado un antivirus actualizado con la licencia vigente, o por haber ingresado a la página del banco en forma no segura por intermedio de algún motor de búsqueda (Google u otros).

Ante esta situación estamos en una disyuntiva si el phishing es un delito informático o una estafa por qué el fin es el hurto del dinero que se encuentra en la cuenta de ahorros o en la tarjeta de crédito.

Por tal motivo no hay una legislación que proteja a la víctima del phishing ya que las entidades bancarias y muchas veces INDECOPI, determina responsabilidad en el cliente.

Pero las entidades bancarias tienen la obligación de:

a) Realizar la ciberseguridad de sus sitios web que se encuentran en el ciberespacio para proteger a sus clientes de las diferentes clases de virus y malware como son el pharming, phishing o defacement, que son elaborados muy técnicamente por ciberdelincuentes a nivel mundial.
b) Detectar, neutralizar y eliminar en los motores de búsqueda (Google y otros) los sitios web con indicación BBVA, con la finalidad de evitar que sus clientes entren a páginas clonadas y sean víctimas de fraudes informáticos con el uso de la información reservada de sus cuentas o tarjetas de créditos.
c) El Banco tiene conocimiento que sus miles de clientes todos no tienen conocimientos básicos de informática, o el uso de la tecnología aplicada a los

teléfonos celulares asimismo tiene clientes de todas las edades desde muy jóvenes hasta adultos mayores y estos últimos son muy susceptibles de ser víctimas de actos delincuenciales en agravio de su patrimonio bajo el cuidado y administración del banco.

Alvarez, N. (2021), los efectos que genera la ineficacia normativa contra la protección a las víctimas de phishing se evidencian en el día a día de esta coyuntura social que resaltó estos casos con los bonos del gobierno, aunado a ello el desconocimiento de la norma hace que las entidades estatales interpreten de manera errónea esta modalidad confundiéndolas con estafas.

Vilchez (2021), que debería ver más conocimientos en informática por parte de las personas porque muy fácilmente hacen transferencias tecnológicas sin tener el total conocimiento de la informática, por ello es importante que las autoridades estén más atentos a estos señores denominados HACKER y por ello con la intervención policial deberá desarticular esta organización criminal que tanto daño hace a los usuarios del sistema bancario.

Paredes (2021), nos dice que, en realidad, no es por la falta de normativa, sino lo que pasa es que esta modalidad delictiva afecta directamente a los bancos y sus clientes, siendo así que ellos mismos se encargan de su investigación actualmente apoyados por la policía especializada, pero a medida que avanza la tecnología siguen apareciendo modalidades conexas, pero si cabe que se actualicen las normativas legales al respecto.

Del Rio (2021) manifiesta, impide una eficaz y adecuada represión de estas conductas lo cual origina desprotección de la actividad económica y empresarial. Viéndose menoscabado el justo derecho de las víctimas a la adecuada preservación de los datos de identidad.

Moran (2021) señaló, en la actualidad uno de los objetivos de la norma (prevenir) no ha sido cumplido, pues no se han efectuado los mecanismos idóneos para la protección de datos de las personas en entidades financieras. Así mismo, como el fraude informático propiamente dicho previsto en código penal y en la Ley 30096 es abarcado de manera amplia, generando vacíos legales que permiten que las entidades no se hagan responsables por el aseguramiento de los datos de clientes.

Luego, ante la formulación de la pregunta, **¿considera que la regulación vigente es eficiente para contrarrestar en los delitos de phishing?**, los expertos explicaron lo mostrado a continuación.

Segundo (2021) indicó, no porque el phishing es cometido por organizaciones criminales bien organizadas; además la regulación no es precisa y no indica las modalidades; por ello, estas organizaciones ilícitas crecen en su logística y generan un peligre latente cada vez más grande .Debiéndose regularizar la norma para que las entidades bancarias faciliten las informaciones de manera rápida solo con la fragancia del delito o con una disposición fiscal para luego confirmar esta disposición por el juzgado respectivo.

Borda (2021), según la legislación contempla que el sujeto activo utiliza un medio tecnológico para realizar estafar financieras a personas que aceden a dichos servicios para la satisfacción de una necesidad al encontrarse un vacío normativo en la identificación del sujeto pasivo trae consigo una deficiencia de identificación del sujeto que ha efectuado el delito informático, por lo que existe un vacío legal, a su vez tampoco existe una normatividad administrativa que regule de manera técnica la búsqueda e identificación del autor material que ha cometido el ilícito penal del delito informático.

Tripi (2021), no existe el delito de phishing, es una modalidad de fraude informático. En materia penal la represión no implica un efecto de prevención, la razón de que la normativa establezca penas ínfimas se denota una ineficiente política criminal relacionada al cibercrimen, considerando además que el Estado peruano es por lo pronto, ineficaz para la atención de los casos, toda vez que solo existe una división especializada de la policia DIVINDAT y no tiene homólogos en el Ministerio Público (que conozcan de la especialidad), hecho que genera un problema mucho mayor.

Pozo (2021), No es para nada eficiente ya que el phishing, es cometido por organizaciones Criminales muy bien constituidas y organizadas y cada uno tiene un rol definido desde el CRAKER que envía el virus, otros miembros se encargan de la parte logística, inmuebles maquinas computadoras conseguir internet, otro

delincuente se encarga de captar a las cuentas receptoras o beneficiarias denominadas MULAS, otro se encarga de recibir y administrar el dinero y finalmente la cuenta receptora o mula quien es la encargada de proporcionar su tarjeta electrónica bancaria para el retiro de dinero y si es una cantidad fuerte este sujeto se persona a la ventanilla del banco y retira el dinero que posterior es entregado al miembro de la organización criminal.

Ante estas circunstancias la pena debe ser más drástica y debe ser investigado por organizaciones criminales o bandas criminales, asimismo se debe regularizar la legislación para que las entidades bancarias proporcionen las informaciones en forma inmediata solo con la fragancia del delito o con una disposición fiscal para después convalidar esta disposición por el juzgado respectivo, teniendo en cuenta que es muy importante capturar a la cuenta receptora en fragancia para que de esta manera identificar a los demás miembros de la organización o banda criminal, generalmente se identifica a la cuenta receptora más a los otros delincuentes.

Zabarburu (2021), nos dice que no es suficiente, pero es una de las armas legales con el que se cuenta a la fecha para hacer frente al fraude informático, y poder frenar el cibercrimen que se viene incrementando a través de sus diversas modalidades.

Alvarez, N. (2021), sobre la regulación vigente es preciso indicar que esta no es eficiente, toda vez que a pesar de señalar las acciones ilícitas que conllevan a una sanción penal, no establece todas las modalidades de los delitos cibernéticos e incluso resalta para muchos abogados una ambigüedad de la norma al no reconocer semejanzas entre delitos informáticos y cibernéticos, dejando de lado las modalidades que han ido apareciendo progresivamente en nuestro país.

Vilchez (2021), que en relación a este punto si bien es importante las penas , para mi concepto el aumento de las penas no es la solución al problema , lo que debería realizarse es un estudio minucioso y poder encontrar una solución a los problemas informáticos , es por ello que el gobierno central debería de dar mayores alcances y conocimientos tecnológicos para el mayor conocimiento de los mecanismos de la tecnología y así poder ayudar a la sociedad de esta lacra social que tanto daño hace a nuestros usuarios

Paredes (2021) señala que la vigente no, por cuanto siguen apareciendo delitos conexos directamente vinculados al phishing, tanto es así que diferentes entidades han tomado nota y han elaborado planes o directivas para contrarrestar este tipo de delitos.

Del Rio (2021) considera que la regulación no es eficiente porque, prescinde precisamente del factor engaño y lo induce a error para el acceso privilegiado a información de carácter reservada. Escenario subsumido en la modalidad del phishing.

Sobre, la interrogación **¿considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?**, los especialistas en delitos informáticos revelaron:

Segundo (2021) indicó, si las leyes impuestas son semejantes a la legislación existente en el convenio porque al ser parte tiene una legislación homogénea entre los demás países miembros, pero esto no se ajusta a la realidad, además que hace falta de políticas públicas.

Borda (2021) señaló, de que se necesita una mayor precisión sobre le identificación del sujeto activo que comité el ilícito penal.

Tripi (2021) manifestó, el Estado peruano para poder suscribir el Convenio de Budapest, tuvo que incorporar y adecuar en su legislación lo relacionado al cibercrimen.

Pozo (2021), si la Ley 30096 y su modificatoria Ley 30771, son idénticas a la legislación existente en el convenio de Budapest y esto tiene una razón de ser ya que un país sea miembro de este convenio tiene que tener una legislación homogénea entre todos los países miembros y está estipulado en este convenio.

Alvarez, N. (2021) dice, que actualmente nuestro país se encuentra suscrito al Convenio de Budapest y si han sido consideradas en nuestro marco legal, sin embargo, la realidad es la falta de capacitación del personal judicial y policial que observan estos casos, asimismo no se ha considerado al detalle las diferentes

figuras de delitos cibernéticos y mucho menos se ha conceptualizado concretamente estos actos ilícitos.

Vilchez (2021) expresó; a mi concepto como abogado litigante, no lo han tenido en cuenta al momento de calificar el presente convenio, porque está vulnerando varios derechos como por ejemplo el ayudar a las personas a personas a poder manejar el sistema informático de una manera no muy usual, y el estado debería de ayudar a las personas a poder manejar este programa ya que muchas personas son víctimas de fraudes informáticos entre otros.

A continuación, se describieron los resultados del instrumento de la ficha de análisis de fuente documental, para ello, se consideró: Jurisprudencia internacional, derecho comparado, informe de análisis estratégico, artículo informativo en página web, resolución de la Fiscalía de la Nación.

En ese sentido, respecto al **objetivo general** que es: Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020. Se analizaron como **fuentes documentales**, los siguientes.

ANÁLISIS DE JURISPRUDENCIA INTERNACIONAL

En la presente jurisprudencia internacional, respecto al **punto tercero y el fallo impuesto en el procedimiento penal – apelación del procedimiento abreviado por el Consejo General del Poder Judicial de Logroño de España (SAP LO 233/2014)** que versa sobre la sentencia del Juzgado Penal de Logroño; nos enfocaremos en el señor Lorenzo quien ha tratado de desvirtuar su accionar indicando que hubo una mala aplicación del artículo 248.2 a) del Código Penal, manifestando que no efectuó ninguna manipulación informática ni ha conseguido una transferencia no consentida, así mismo dijo que se vulneró su derecho a la presunción de inocencia, de esto señalamos que resulta impropio y carece de veracidad dado que se demostró que el autor tiene conocimiento de la propia acción y las consecuencias que genera dicho acto.

Pero, conforme la jurisprudencia la Sala ha indicado en el tercer párrafo del punto tercero de la sentencia sobre apelación del procedimiento abreviado que no está de acuerdo con la calificación de cooperador necesario de un delito consumado; ya

que el acusado no consumó el delito de acuerdo a los actos descritos y lo establecido en la norma de España. Por ende, las acciones ilícitas realizadas por el autor configuradas en la aplicación de las normas en los casos de modalidades de phishing, se puede concluir que en el presente caso del señor Lorenzo existió una ineficacia normativa; ya que, la norma impuesta para el acto ilícito efectuado por el acusado era específica y concreta, pero no fue eficaz; toda vez que el administrador de justicia que impuso la sentencia en el Juzgado Penal, no consideró el grado de tentativa y la pena impuesta en el artículo 62 del Código Penal; evidenciando la falta de conocimiento legal, interpretación de la norma, y los efectos legales de la ineficacia normativa, que en este caso correspondió a una pena de prisión como autor responsable de un delito de estafa informática en modalidad de phishing, cuando debió de especificarse el grado de tentativa al entregar el acusado el dinero sustraído del banco.

ANÁLISIS DE DERECHO COMPARADO

El análisis de derecho comparado realizado, evidencia la necesidad de modificar la ley incluyendo en forma expresa los delitos informáticos contra el patrimonio, haciendo factible que haya distinciones entre las modalidades, a fin de que se pueda proteger y defender a las víctimas de estos delitos que se desarrollan por un sistema informático como es el caso del phishing.

Ahora bien, **España** ha implementado de forma armónica en el **artículo 248. 1. de la Ley Orgánica 10/1995** la figura de estafa enfatizando los actos que serán materia de sanción; pero, también empleó otras figuras clásicas penales con el fenómeno informático, adoptando la aplicación de leyes especiales con la finalidad de hacer frente al problema de la criminalidad informática.

Asimismo, **Alemania** ha introducido en su legislación el **artículo 263.a del Código Penal Alemán** y complementario a ello usaron nuevos conceptos penales para la represión criminalidad informática, para ello su gobierno tuvo que reflexionar sobre la problemática actual y verificar si la aplicación del Derecho Penal tradicional era suficiente para reprimir esas nuevas acciones que generan nuevos lesiones a bienes jurídicos que era merecedores de protección, aclarando que de nuestra consideración aún falta indicar y mejorar los medios empleados en estos delitos; ya

que, el computador no es la única forma de obtener una ventaja patrimonial en esto casos, por el cual se debe enfatizar las diversas modalidades que han ido surgiendo.

En Ecuador, el artículo 190° del **Código Orgánico Integral Penal**, si bien señala las acciones ilícitas que serán sancionadas, observaremos la carencia en identificar las modalidades en estos delitos informáticos, lo cual sumado a la realidad del país veremos la deficiencia en sus administradores de justicia que va en conjunto a leyes impuestas sin conocerlas.

Por su parte **Chile** no contempla en el **artículo 2° de la Ley Nº 19.223** las nuevas figuras de delitos informáticos como hacking o el fraude informático, de esto modo esto evidencia las falencias en los que incurre su legislación respecto a la regulación de estos delitos, dejando un vacío en la interpretación sobre el significado del sistema de tratamiento de información, sin considerar los medios empleados o especificar adecuadamente la acción punible.

Por último**, Perú** también muestra esas deficiencias en el artículo 8° de la Ley Nº 30096 dado que no permite de forma eficiente imponer un castigo efectivo para los comportamientos ilícitos, ya que en el concepto de fraude informático agrupa todas las posibles modalidades ilícitas sin diferenciarlas y ocasionando ineficacias normativas al emplear la norma o al momento de formulación de la denuncia, generando como efectos el archivamiento, falta de individualización del autor, sobreseimientos por malas aplicaciones en el recojo de la evidencia digital, entre otros.

Objetivo específico 1 “determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa”.

Respuestas de los expertos entrevistados.

Al preguntarles sobre, **¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa?** los expertos dieron como punto de vista lo declarado a continuación.

Segundo (2021) indicó, se vulneran a estas víctimas con la falta de ejercer bien la administración de justicia, ya que no se encuentra la responsabilidad en quien

ejecuta dichos actos, sino todo lo contrario, el cliente de la entidad bancaria sale perjudicado y no existen muchos especialistas en estos temas que lo puedan asesorar.

Pozo (2021) respondió, la ley sanciona la comisión de los delitos informáticos y el hurto de dinero con el uso de la modalidad de phishing, las entidades financieras son las que no asumen responsabilidades y solo responsabilizan al cliente, esta respuesta tiene mucho que ver con lo que respuesta en la primera pregunta.

Alvarez, N. (2021) dijo, la vulneración de protección a las víctimas de phishing se realiza cuando no se respeta el bien jurídico protegido de toda persona, en estos casos se hace mención al patrimonio, integridad, confidencialidad y disponibilidad de información de las víctimas, quienes se perjudican y pierden la confianza en el sistema judicial para la resolución de estos delitos; ya que, el presunto denunciado tiene acceso a sitios web que perjudicarían al denunciante y al no ser procesado por falta de pruebas, mala formulación de denuncias o pericias mal ejecutadas; todo ello conllevaría a la falta de protección de políticas públicas en estos delitos.

Moran (2021) planteó, a la fecha las entidades financieras no han generado una protección adecuada de los datos de los clientes, por cuanto no existe una sanción para ellos, la norma si bien tiene como objeto prevenir el delito, esto no se ha cumplido, debido también a las innovaciones tecnológicas que se implementan para los hechos delictivos.

Cuando se planteó la pregunta, **¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?** dijeron lo suscrito en los siguientes párrafos.

Segundo (2021) indicó, sí, porque esto permitirá identificar al autor del acto delictivo conforme a la manera de escoger a sus víctimas. Incluso, los datos de cifras actualizadas y categorizadas llevarían a ver el margen de crecimiento y los formas de contrarrestar estas modalidades.

Borda (2021) manifestó; que si, es necesario categorizarlo dado que los delitos informáticos pueden abarcar lesiones contra el patrimonio, libertad sexual y otro.

Alvarez, N. (2021) en base a su experiencia fijó su atención en las cifras explicando; sí, es necesario tener un amplio panorama de las cifras actuales de estos hechos delictivos que permitirían prevenir e identificar quienes son las personas más vulnerables a ser víctimas, así también se diferenciaría cada modalidad y esto conllevaría a conceptualizar mejor para realizar sanciones concretas y específicas; ya que la DIVINDAT, solo tiene datos generales en base a las denuncias formuladas más no existe cifras de cada modalidad cibernética y en muchos casos son confundidas con la figura delictiva de estafas.

Formulada la cuestión, **¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MPFN?**, señalaron lo consignado en los siguientes acápites.

Segundo (2021) indicó; sí, deben hacerse cambios en la legislación y especificar las modalidades, para permitir la identificación adecuada del autor y una acusación del hecho punible acorde a la norma. De esta manera, las personas que son víctimas de phishing, estarían más protegidas ante la actuación de los administradores de justicia que muchas veces cometen errores en la imputación del delito.

Borda (2021) señaló; que, si consideramos necesario, que en la Ley se tiene que implementar, pero normas de carácter de la especialización y que coadyuvan a una mejor investigación del Ministerio Público.

Pozo (2021) sugirió, en la Ley 30086 y su modificatoria, se deben hacer cambios en la legislación y ser más específicos como estipular que el delincuente con el uso de la información reservada de tarjetas o cuentas bancarias y la vulneración de claves secretas realiza transferencias ilícitas de dinero vía internet comete delito informático. De esta forma la persona que son víctimas de phishing, estarían más protegidas.

Alvarez, N. (2021) prefirió responder expresando que, la Ley N°30096 debe ser modificada porque como bien mencioné anteriormente no precisa el concepto de estas modalidades y mucho menos aclara la diferencia entre delitos informáticos, cibernéticos y estafas; además, debe considerarse capacitar al personal judicial y

policial, que muchas veces desconocen de estos temas y se encuentran laborando en el área de ciberdelitos.

Del Rio (2021) considera, en un marco irrestricto de atención al principio de legalidad, se debe procurar que conductas como las enunciadas se encuentren preestablecidas en un dispositivo con rango de ley, más aún, si en la actualidad representa una de las técnicas más empleadas para hurtar información a través de internet.

Por otro lado, se ha descrito las **fuentes documentales** correspondientes al **objetivo específico 1**, el cual es; determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa. Para ello se sometieron a análisis las fuentes documentales que a continuación se describen en el siguiente apartado.

ANÁLISIS DE INFORME ESTRATÉGICO

El análisis estratégico en el **acápite II de Estadísticas Oficiales del punto 2.1. al 2.3**. elaborado por La División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT), expone la necesidad de implementar mecanismos eficientes y tecnológicos. Además, se debe tener en cuenta el equipamiento tecnológico necesario, así como el personal capacitado con la finalidad de permitir la lucha eficiente contra estos delitos que son de mera importancia por el grado de incidencia en los que se comete.

Dicho esto, podemos identificar el alto nivel de vulnerabilidad de cualquier ciudadano para ser víctimas de delitos informáticos, con el análisis estratégico observaremos que no existen cifras categorizadas por modalidades de este delito, es decir, no tenemos certeza de la cantidad de víctimas de phishing; resaltando la falta de protección del bien jurídico protegido en estos delitos establecidos en la ley y la ausencia de políticas públicas para proteger legalmente a las víctimas de phishing en entidades financieras, no solo en procesos penales sino también en el fuero administrativo, ya que las leyes nacionales mencionadas en esta fuente no son eficaces teniendo como resultado altos registros de denuncias.

ANÁLISIS DE ARTÍCULO INFORMATIVO EN PÁGINA WEB

Este artículo informativo en página web sobre la **nota informativa** de detención a integrante de banda en primer caso de delito informático con investigación fiscal especializada, muestra que el Estado a través de la normatividad jurídica ha planteado la problemática de los delitos informáticos, creándose la Unidad Especializada en Delitos Informáticos con propósito de investigar de forma diligente estas figuras delictivas, facilitando la persecución y sanción de las conductas ilícitas que lesionan los sistemas y datos informáticos.

Además, el artículo antes mencionado aprecia el inicio de investigación preliminar a fin de poder individualizar a los sujetos que perpetuaron el ilícito, sin embargo podemos concretar que la víctima de esta modalidad de delito informático hasta el momento no ha podido recuperar su dinero y la entidad bancaria por el cual se efectuó las transferencias no ha realizado ningún pronunciamiento, quedando nuevamente a la deriva la protección a las víctimas de phishing en entidades financieras debido a la existencia de una norma que no es eficaz en su empleo y a pesar de la existencia de la nueva fiscalía aún nos faltaría expresar claramente las modalidades que se pueden presentar del fraude informático para evitar errores con los casos de estafas.

ANÁLISIS DE JURISPRUDENCIA INTERNACIONAL

La presente jurisprudencia internacional versa sobre la Causa N°36742/2011. 24/10/2013 en base a la **decisión efectuada por la Cámara Nacional de Apelaciones en lo Criminal y Correccional – Sala V;** que refiere los parámetros de la actuación criminal en defraudación por medios informáticos, como modalidad el phishing, planteando la importancia del dolo en estos actos delictivos realizados en Barcelona.

En consecuencia, debemos tener en cuenta el contexto actual en que vivimos; ya que, esto evidencia el abandono de los administradores de justicia ante el vacío para identificar e individualizar correctamente a los verdaderos autores del delito, siendo esencial la actualización digital. Entonces, según el fallo de la Cámara Nacional de Apelaciones en lo Criminal y Correccional el nivel de participación es distinta si no se tiene conocimiento de los planes del autor, esto incurriría en la falta

del dolo como instrumento y no existiría autoría mediata, puesto que en el caso los partícipes actuaron de acuerdo a una simulación de contrato y fueron inducidos a error mediante un engaño para conseguir el apoderamiento patrimonial de forma indebida, perjudicando a los auténticos titulares de las cuentas bancarias (víctimas de phishing) quienes fueron vulnerados en la protección de sus datos, afectándolos económicamente; enfrentándose a una norma que no es eficaz en su empleo, por la falta de identificación del autor que al parecer empleó virus informáticos y contrataciones simuladas de agentes de transferencia de dinero tratándose de una estafa masiva. Si bien concordamos con la decisión tenemos que criticar la ausencia nacional e internacional para obtener justicia para las víctimas de phishing entre otras modalidades, pues los medios y el personal no está capacitado para enfrentar estos casos.

Por último, respecto al **objetivo específico dos** que es, "identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras".

Respuestas de los expertos entrevistados.

Sobre la pregunta, **¿de qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?**, los entrevistados explicaron lo siguiente.

Segundo (2021) indicó, la actuación del Ministerio Público se ha visto en la creación de la Nueva Fiscalía Especializada en Ciberdelitos; sin embargo, falta la capacitación del personal para poder interpretar la norma y aportar ayuda a las víctimas de estos delitos. Además, a ello se suma que esta fiscalía no es suficiente para todo el país.

Borda (2021) manifestó, el Ministerio Público dentro de sus funciones está la de investigar un hecho delictuoso aplicando lo establecido en el Código Penal y su Ley orgánica, para la identificación de víctimas de phishing en entidades financieras se hace necesario la presentación de un proyecto de ley que la misma que puede ser por la máxima de la experiencia por los casos que se vienen investigando, donde se evidencia las falacias normativas y ser más eficaces para la resolución del delito.

Pozo (2021) expresó, que el Ministerio Publico al tener una fiscalía especializada se capacite y trabaje en forma conjunta con la PNP y más que todo aprovechar la flagrancia en esta modalidad.

Alvarez, N. (2021) precisó, el Ministerio Público, ha buscado contrarrestar estos delitos creando una nueva fiscalía, la cual es la única a nivel nacional que en la realidad no se abastece y además desconoce de la realidad problemática, así como el personal no está calificado por falta de especializaciones, conocimientos informáticos y legales.

Del Rio (2021) sostuvo, con el desarrollo de nuevas tecnologías ha surgido un incremento de la ciberdelincuencia, para este efecto el ministerio ha creado la Unidad Especializada en dicha materia, procurando desde una orientación técnico jurídico en la investigación, la preservación de la evidencia digital, aplicando y proponiendo directivas, lineamientos, instructivos y guías en el marco de su competencia.

Al preguntarles, **¿qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?**, comentaron los siguientes puntos de vista.

Segundo (2021) indicó, la implementación de despachos fiscales sería una actuación muy eficiente, si se suma con ello las capacitaciones y un presupuesto adecuado para que se mantengan actualizados tanto el aporte humano como el material. También, es preciso requerir de peritos informáticos, los cuales permitirán una identificación del autor (phisher) para la respectiva individualización, evitando con ello el archivo de tantos casos referentes de los delitos cibernéticos.

Según, Borda (2021); que conforme se tiene de la disposición de la Fiscal de la Nación se han creado las fiscalías especializadas en delitos informáticos, empero se ha entendido que dichas solo emiten opiniones para la investigación las mismas que son realizadas por las fiscalías comunes, a su vez se tiene que tomar en cuenta de la gran cantidad de hechos punibles cometidos por los sujetos activo del delito informático, estos casos se han incrementado, por lo que debería de darse el

verdadero significado y especialización a dichas fiscalías dado que son los únicos que podrían investigar los delitos informático.

Tripi (2021) explicó, la administración de justicia se encuentra en sede del Poder Judicial, respecto del Ministerio Público, su actuación en cooperación con la PNP es muy importante, siempre y cuando conozcan de la especialidad, como lo mencioné en preguntas anteriores, la PNP no tiene un homólogo en el MP especializado, si bien han creado Fiscalías para asumir la investigación o estrategia legal para la investigación, lo cual, generará siempre un peligro en la adecuada operatividad jurídica de las entidades encargadas.

Pozo (2021) indica, me parece una decisión del Ministerio muy oportuna ya que las transferencias ilícitas de dinero vía internet por la modalidad de phishing, u otras modalidades de dinero son muy técnicas y requieren de personal de fiscales especializados o delo contrario estos crímenes quedarían impunes.

Alvarez, N. (2021) contestó, me parece una gran iniciativa, siempre que el gobierno aporte con políticas públicas y presupuesto para llevar a cabo regularmente las capacitaciones del personal, porque si dejamos de lado esto sería como tener un caballo blanco, inservible para la población.

Del Rio (2021) respondió, que es adecuado para la problemática existente, considerando que desde el 22 de octubre de 2013 al 31 de julio de 2020 ingresaron a la fiscalía un total de 21,687 denuncias por delitos informáticos; cuyo conocimiento correspondían a esta unidad especializada, que por su carácter dotará de mayor eficacia el recojo de indicios y preservación de la evidencia.

Moran (2021) expresó, la especialización de despachos fiscales en delitos cibernéticos hace que se implementen la normativa específica para cada caso y en consecuencia las sanciones sean las adecuadas, así mismo, promueve una estadística de los casos con los que se podrán materializar nuevas normativas que permitan contrarrestar este delito.

Finalmente, al ser consultados sobre si, **¿considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?** sostuvieron los siguientes pronunciamientos.

Segundo (2021) indicó; sí, la educación y la prevención que se debe generalizar en los clientes bancarios y los administradores de justicia, tanto policías como fiscales y jueces; para evitar más víctimas de fraudes informáticos. Teniendo en cuenta que esta responsabilidad de educación no solo recae en el estado, también debe tener participación de las entidades bancarias quienes deberían de preocuparse por la falta de conocimiento de sus clientes ante estos hechos delictivos.

Borda (2021) indica; que, si estamos de acuerdo que el estado pueda difundir sobre los alcances del delito informático, pero a su vez se hace necesario que las entidades financieras también realicen y/o proponen la protección de datos para el uso de los servicios de internet.

Tripi (2021) considero, que toda acciones para mitigar los fraudes cibernéticos deben ser impulsado a nivel privado y estatal, actualmente los bancos se aprovechan de sus limitaciones en seguridad y obligan al cliente a asumir seguros para cobertura de fraudes cibernéticos, esto es un abuso privado que te genera un problema público, pues dejan de lado los casos cibernéticos solo porque ya no son rentables, toda vez que el consumidor final adquirió un seguro que cubrirá el fraude, los más perjudicados son aquellos que no pueden adquirir dicho seguro.

Pozo (2021) manifestó, si claro es la educación y la prevención que se debe internalizar en los clientes bancarios para evitar ser víctimas de fraudes informáticos por medio del phishing.

Zabarburu (2021) indicó, la prevención es importante para dar a conocer a la ciudadanía que cada vez es más digital de los peligros al que está expuesto y modalidades existentes al que recurre el ciberdelincuente para obtener información confidencial.

Alvarez, N. (2021) sostuvo, que si podría ayudar sobre la educación de prevención a la población sobre estos hechos; sin embargo, la interpretación de la norma se rige en base a nuestros administradores de justicia y son ellos quienes también deben recibir la información correspondiente en base a la Ley N°30096. Además, centrándose en la modalidad de phishing debe considerarse que las entidades financieras también forman parte de estos hechos, en algunas ocasiones

son víctimas y otras veces son utilizadas como medio de suplantación por otros sitios web, es así que debe considerarse una política al usuario de prevención ante estos hechos.

Del Rio (2021) señaló, que una adecuada educación tecnológica garantiza el carácter preventivo de la norma y como consecuencia de ello, tendrá más efectiva su eficiencia, ampliando en un ámbito técnico la tipicidad de la conducta.

Se analizaron como **fuentes documentales**, las siguientes fichas de fuente de análisis documental.

ANÁLISIS DE RESOLUCIÓN DE LA FISCALÍA DE LA NACIÓN

La resolución de la **Fiscalía de la Nación N°1503-2020-MP-FN,** según la **parte resolutoria, artículo Tercero,** inciso 6; planteó las funciones que realizaría la Unidad Fiscal Especializada en Ciberdelincuencia; destacando la promoción de articulación de dos entidades tan significativas como el Ministerio Público y la Policía Nacional, teniendo en consideración el brindar un acompañamiento técnico a los fiscales en la realización de la investigación de los delitos previstos en la Ley de delitos informáticos.

Es así, que consideramos importante esta actuación del Ministerio Público; ya que, consolida los criterios planteados en los procedimientos y métodos de investigación en materia de ciberdelincuencia buscando orientar a los fiscales penales en la realización de investigación dando frente a la ineficacia normativa, falta de políticas públicas, mala interpretación de la norma. También trata de vincular como en otros países se ha ido ejecutando y ha funcionado cabalmente ante la lucha de los nuevos delitos informáticos, recordando que el principio de cooperación efectuado entre los países debe emplearse congruentemente con el manejo de cada ministerio buscando unanimidad para obtener un empleo de justicia eficiente en diversas materias legales.

ANÁLISIS DE JURISPRUDENCIA INTERNACIONAL

La jurisprudencia internacional hace mención al **artículo 8° del Convenio de Budapest**; el cual define los delitos informáticos como la acción de introducir,

alterar, borrar o suprimir datos de esta índole, agregando cualquier interrupción en un sistema informático.

Se debe precisar que en general el convenio conceptualiza al sistema informático como cualquier dispositivo aislado o grupo de dispositivos conectados o relacionados entre sí, cuya función de cualquiera de sus elementos es el procesamiento automático de los datos de ejecución del programa. Por ende, para buscar una definición sobre los delitos informáticos se requiere muchas veces que esta conceptualización este en la normativa punitiva, sin embargo, la normativa peruana no establece en si una definición de delitos informáticos, solamente regula de forma general, ocasionando posturas legales diferentes entre delitos cibernéticos, delitos informáticos y estafas.

Aunado a ello, podemos finiquitar indicando que el trabajo del Ministerio Público se ha venido asociando conforme a este convenio, puesto que todos sus informes, proyectos describen en su normativa extractos del Convenio de Budapest para contrarrestar los delitos informáticos.

Discusión. - En el presente apartado se estudian y valoran los hallazgos obtenidos de los instrumentos aplicados, ordenada primero, a la crítica de los resultados en base al que tuvo mayor consistencia conceptual y legal; segundo, se sujetará al contenido formulado con coherencia. Lo señalado, manifiesta y evidencia la teoría obtenida que si bien estará dividida en dos partes ayudará al mejor proceder para el desenvolvimiento de la discusión.

En base a lo descrito, se reitera que la estructura de la discusión estará acorde al orden del trabajo, esto es, primero los objetivos, desde el general a los específicos uno y dos. Además, si bien la finalidad de este trabajo no es admitir o rechazar los supuestos, que son las posibles respuestas del problema, se debe recordar la utilidad e importancia del supuesto general que permitirá revelar si la primera contestación fue la adecuada o no, evidenciando el avance de la investigación.

Es así, que la discusión comenzará con la exposición del objetivo y junto con ello la remembranza del supuesto; por ello se presentará en las siguientes tablas.

Objetivo general
Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.
Supuesto general
La ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima; generó como principales efectos, la falta de seguridad informática y daños patrimoniales; porque el usuario, consumidor o también denominado víctima, se encontró con discrepancias en el tratamiento de las leyes penales.

Posterior de la revisión del estudio, de ellos, se planteó como la mejor manera de entender y dilucidar la conceptualización de la ineficacia normativa, en base a conceptos impartidos en la doctrina y la ley. Aparentemente, esto no englobaría la falta de protección a las víctimas de phishing; sin embargo, se debe recalcar que la resolución del problema general, objetivo general, desprende del concepto de ineficacia normativa concerniente a la modalidad de phishing dentro del marco normativo penal del fraude cibernético; ya que, los hallazgos de los resultados puede ser el caso que contradigan algunas tesis citados en el marco teórico.

En ese sentido, Pardo (2018) mencionó, que la regulación jurídica en el ámbito penal es inconsistente, todo ello partiendo de la afectación informática contra el patrimonio en diversas tipologías delictivas de ciberdelitos que generan inseguridad en la exégesis, respecto al empleo legal en materia penal de delitos cibernéticos siendo ineficaz, por la falta de claridad y expresa la vulneración al patrimonio por medio de sistemas informáticos. En concordancia con él, Zorrilla (2018) concluye , que existió una evidente imprecisión de acuerdo a la redacción que generó confusión e incertidumbre en relación a la Ley Nº30096 y la Ley Nº3017 que la modifica, ocasionando desconciertos entre las partes procesales y limitó en cierta forma las formulaciones de denuncias o logró que el agente activo de este delito no se encuentre, imposibilitando que se sancionen a los verdaderos culpables. Concerniente a ello, el significado de ineficacia normativa atañe la inadecuación de la ley por parte de los miembros de diversas instituciones creadas para administrar

justicia, porque la ley estipulada para esta materia no es precisa (autores citados en el marco teórico).

En consiguiente, el marco legal sobre delitos informáticos en la modalidad de phishing está conformado por Ley Nº30096, y su modificatorio Ley Nº30171, que resalta como bien jurídico al patrimonio, integridad, confidencilidad y disponibilidad de información y simultáneamente el DL Nº635, modificado por el DL Nº1237, DL Nº1182 y Ley Nº28493; todas ellas siendo nomas establecido de forma general sin guiar una tipificación concreta que recoja las falencias encontradas.

Asumiendo estas posturas y en concordancia con los resultados obtenidos del objetivo general, existe ineficacia normativa toda vez que al no haber una legislación que proteja a la victimas del phishing entre otras modalidades de delitos informáticos, la responsabilidad total recae en el cliente; aunado a ello el desconocimiento de la norma hace que las entidades estatales interpreten de manera errónea estas modalidades confundiéndolas con otro tipo penal. También, se debe precisar que el caso en concreto de la modalidad de phishing el cual se encuentra tipificado como fraude informático, la norma dispuesta no permite una eficaz y adecuada represión de estas conductas originando la falta de seguridad jurídica a la actividad económica y empresarial, faltando gravemente a uno de los objetivos principales de la norma, el cual es de prevenir; generando de esta manera la ineficacia normativa, siendo esto un camino fácil para las organizaciones criminales que crecen en su logística y son un peligro latente al mostrar ambigüedades, no reconocer las diversas manifestaciones de actos ilícitos e induciendo a error para el acceso privilegiado de información reservada.

A partir de ello, conforme la jurisprudencia internacional, observaremos que cada país a tipificado de manera diferente, en base a su realidad problemática; donde muchas veces trasluce la falta de conocimiento legal, deficiencias de la norma, y los efectos legales de la ineficacia normativa, como en el caso expuesto en la fuente de análisis documental que impusieron una pena de prisión distinta al delito de estafa en grado de tentativa en la modalidad de phishing. Donde el análisis de derecho comparado, muestra la necesidad de modificar nuestra ley incluyendo en forma expresa los delitos informáticos contra el patrimonio en sus distintas modalidades, para proteger y amparar a las víctimas de estos delitos.

Por lo tanto, la ineficacia normativa del phishing da a conocer a todos los individuos que son vulnerables en el sistema informático y que son responsables totalmente las empresas financieras que se aprovechan de los clientes y la mala estipulación de la norma; por falta de conocimiento legal y su uso abusivo de seguros que recaen en los clientes. Comprendiendo un delito por que son acciones que se ejecutan con intensión de transgredir el patrimonio de la víctima; es por ello, que la tipificación o establecer reglas legales para luchar contra el fraude informático y todas sus modalidades es imprescindible para la adecuada protección a las personas vulnerables, considerando que la prioridad de la norma es mantener el control sobre la conducta de la persona en busca de un bienestar social, además el iusnaturalismo y las máximas de la experiencia nos ha mostrado que el tipificar correctamente una acción que ha repercutido en muchos daños para otras personas trae como consecuencia el desarrollo de la nación en todas sus dimensiones, restando las cifras de delitos. Es así, que vamos a mencionar el carácter transnacional del fraude informático, que ha venido acarreando diversos problemas para identificar al autor de estos tipos delictivos, resaltando la necesidad del principio de cooperación no solo de las entidades públicas de nuestro país, sino también del aporte internacional.

Objetivo específico uno
Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa.
Supuesto específico uno
La protección a las víctimas de phishing en entidades financieras, se vulneró al no respetar el derecho de estas personas y por el mal actuar de los administradores de justicia; lo cual, fue evidenciado con las denuncias.

Para comprender la vulneración de protección a las víctimas de phishing en entidades financieras, es importante tener en cuenta que, si bien la norma no es eficaz esto conlleva a la falta de protección jurídica para todo individuo que se vea perjudicado sobre estos delitos. Reyes (2020) recomendó que se logre realizar un trabajo conjunto con los operadores de justicia y apoyen a las víctimas de diferentes variantes de delitos informáticos, con el fin de lograr la detección temprana,

orientación y ejecución, los manejos de protocolos de seguridad de manera de que dichas personas puedan actuar diligentemente en sus acciones legales, policiales y penales correspondientes a su defensa de su integridad personal y el derecho de tutela. En concordancia con el autor sobresale Abdulai (2016) quien relacionó el uso del internet y el riesgo de convertirse en víctima de fraudes con tarjetas de crédito o débito, ya que existe un riesgo al efectuar transacciones mostrando que se puede realizar una clasificación de las víctimas (autor citado en el marco teórico).

Es así, que es indispensable aclarar la definición conceptual de víctimas de phishing, el cual, trasciende de la población afectada por este delito informático que abarca sistemas o redes, siendo generalmente mal clasificados según su tipo penal; asimismo, este individuo es determinado como el sujeto pasivo (persona natural o jurídica) que desconoce de tecnología.

En este punto, es pertinente mencionar que, de los resultados obtenidos, la mayoría de los especialistas concordaron en que sí se vulnera a las víctimas, esto se suele dar por falta de buena administración de justicia, inexactitud al plantear el tipo penal y desconocer el bien jurídico protegido perjudicado, inadecuada sanción penal y sobre todo carencia del respeto al principio de legalidad; ya que, en muchas ocasiones no se ejecuta lo que dicta la norma. También, se observa la incertidumbre del cliente de una entidad bancaria o víctima que no encuentra ningún tipo de asesoramiento, perjudicándose y perdiendo la confianza en el sistema judicial.

En consecuencia, es indispensable la implementación de mecanismos eficientes y tecnológicos como se muestra en la fuente de análisis documental; pues así, sería una manera de contrarrestar la vulnerabilidad que tiene cualquier ciudadano para caer en víctimas de estos ciberdelincuentes; además, las políticas públicas bien ejecutadas aportarían en la educación ciudadana e individualización del sujeto activo. Es cierto, que existe una investigación preliminar sobre todo que actualmente lo viene realizando la Fiscalía de la Unidad Especializada en Delitos Informáticos, sin embargo veremos diferentes casos que han quedado a la deriva incluso en jurisprudencia internacional donde se plantea la importancia del dolo en estos actos delictivos; ya que muchas veces el autor del delito utiliza a otros

individuos empleando el engaño y estos se hacen partícipes del delito sin tener conocimiento alguno e intención de efectuar un acto ilícito.

Por lo tanto, la sincronización a nivel nacional de administradores reguladores de justicia, permitiría un desenvolvimiento real y visible, para la población, puesto que las faltas de conocimiento normativo agregado a la actuación individual han venido perjudicando a la sociedad. Asimismo, la clasificación del estereotipo del autor del fraude informático en la modalidad del phishing no basta, porque, estos también dividen a sus víctimas; por ello, se debe comprender el pensamiento y la finalidad que buscan estos delincuentes, para de esta manera explicar y recomendar a la población las formas de estar precavidos, implementando actividades que gestionen el gobierno y la administración pública, para redimir lo que necesita la población, educándola sobre la prioridad de la identificación de páginas verificables y confiables para cualquier actividad financiera, evitando ser víctima de la modalidad del phishing.

Objetivo específico dos
Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras.
Supuesto específico dos
El Ministerio Público enfrentó la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras de una manera concreta y productiva; por ello, formó la Unidad Fiscal Especializada en Ciberdelincuencia, porque se observó el incremento de ciberdelitos en la modalidad phishing en la época de pandemia, sin embargo eso no fue suficiente.

Es crucial comprender, que la actuación del Ministerio Público debe estar acorde con la modernización de los ciberdelincuentes; por ello Hidalgo (2018) percibió que el auge de la tecnología conllevó a la creación de los ciberdelitos; por ello, se debe buscar un equilibrio con el marco normativo penal.

Con lo dicho y guiados de nuestro día a día, que vincula la sobrecarga procesal, falta de presupuestos y políticas públicas en base a los delitos informáticos, consideramos la opinión de Borda (2021), pues expresa la función principal del MP,

el cual, es de investigar un hecho punible aplicando el Código Penal y su Ley Orgánica; en concordancia con ello, Del Rio (2021) sustentó que la nueva Unidad Especializada en ciberdelitos realiza la orientación jurídica en la investigación conforme los lineamientos establecidos en la ley. Sin embargo, estas opiniones que son realizadas por las fiscalías no contribuyen en mucho a contrarrestar a nivel nacional estos delitos, ya que falta personal, conocimientos de la normativa y sobre todo que lleguen a Lima y provincias; además no existe un trabajo conjunto con la PNP. Por ello, es necesario impulsar una modificatorio legal basada en la máxima de la experiencia debido a los casos investigados que sacan al aire las falencias normativas, en el cual intervengan el sector público y privado, quitándole esas faltas de limitaciones a los bancos quienes se aprovechan en los cobros de seguros a los clientes. Aunado a ello, es necesario que las entidades financieras realicen y propongan la protección de datos para evitar estos fraudes informáticos en la modalidad del phishing; ya que, la educación tecnológica garantiza el carácter preventivo de la norma y garantiza su eficacia.

Todo lo expuesto, se asocia a la resolución de la Fiscalía de la Nación N°1503-2020-MP-FN, donde se plantea las funciones de la unidad encargada de la investigación de los ciberdelitos; buscando un trabajo concatenado para la lucha de delitos informáticos y por ello, se emplea también el marco internacional conforme el artículo 8° del Convenio de Budapest donde se conceptualiza los delitos informáticos como la acción de introducir, alterar, borrar o suprimir datos, agregando cualquier obstáculo en un sistema informático; la cual es recabada en nuestra Ley N°30096, sin considerar otras modalidades, actos ilícitos que han surgido en los últimos años en el ciberespacio.

Por lo tanto, la actuación del Ministerio Público es crucial para el desarrollo de la lucha contra la ciberdelincuencia, la implementación de una fiscalía si bien ayuda a la investigación no abastecerá todo el ámbito territorial que nuestro país tiene. Dicho esto, complementar normas internacionales sin tener la realidad problemática clara y adherirla no da respuesta ni solución a nada, sino más bien ocasiona vacíos legales, que no permiten a los reguladores de la justicia interpretar correctamente la norma. Para culminar completamente este acápite, mencionaremos que en el transcurso de la investigación, hemos podido aseverar lo señalado en los

supuestos, ya que el Perú aún está encaminado a modificatorias legales de toda índole, entre ellos en el ciberespacio, lugar que muy pocos conocen y muchos se aprovechan de ello, en base a vacíos legales o normas que en el desarrollo de la profesión nos percatamos que son ineficaces y no cooperan a la prevención de los actos ilícitos y mucho menos a la identificación de quienes ejecutan estos hechos punibles.

V. CONCLUSIONES

PRIMERO: Se analizó los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, el cual es ineficaz debido que el fraude informático, se basa en la falta de empleo de la misma y la ausencia de la aplicación de la sanción; por ello, se analizó que la aplicación de la norma es ineficaz ya que, surge controversias en su sanción al no estipular dentro del artículo 8° de la Ley N°30096, titulada como fraude informático todos las modalidades de delitos informáticos que infringen el patrimonio ocasionando un desmedro en la interpretación de la norma que no permite una sanción efectiva. De ello, se puede colegir en concordancia con los expertos y la jurisprudencia internacional, que es necesario la modificación de la norma teniendo en cuenta los diversos avances tecnológicos y los tipos delictivos que han aparecido junto a ello; más aún cuando la norma establecida solo establece de forma general algunas acciones sancionables creando ineficacia normativa en el desarrollo de los casos de esta materia; debido a que muchos abogados discrepan sobre los medios empleados considerados en este tipo penal; dado a la ambigüedad del artículo 8° de la ley en mención, que no es preventiva y no permite una investigación eficiente ocasionando deficiencias en la investigación por la complejidad del modus operandi.

SEGUNDO: Se determinó la vulneración a la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa , dado a que la conducta del delito de phishing informático afecta la esfera patrimonial de la víctima, quien es la persona que sufre la afectación por el delito informático, ocasionado del accionar malicioso del phisher que genera grandes pérdidas económicas haciendo uso de su conocimiento tecnológico, por lo cual, ocasiona una victimización a la víctima, la misma que carece de conocimientos suficientes para poder identificar un portal

web original, y a su vez es necesario identificar las categorías de víctimas para efectuar una investigación satisfactoria. Por lo tanto, es que el Estado debe brindar seguridad jurídica a las víctimas a través de las instituciones encargadas de administrar justicia, para así dar a la víctima el soporte que necesita haciendo uso del goce y ejercicios de sus derechos para poder acceder a la justicia, pero en muchos casos surgen impedimentos a nivel de investigación que limitan que se logre una efectiva sanción quedando en impunidad. Finalmente, es necesario que se brinde a los usuarios que son propensos de ser víctimas, por la falta de conocimiento y cultura informática, campañas de información para poder detectar estos delitos informáticos y saber actuar ante ellos.

TERCERO: Se identificó la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, lo cual es deficiente debido a que las instituciones encargadas de administrar justicia se encuentran desarticuladas y poco coordinadas, ello genera la ineficacia y en consecuencia pierde el propósito de garantizar a las víctimas la protección y sanción, sobre contrarrestar los delitos informáticos quedando en impunidad. Es así que, los límites legales del fraude informático se encuentran establecido en la Ley N°30096 en concordancia con el Convenio de Budapest; por tal motivo la actuación del Ministerio Público a nivel de investigación no es satisfactorio debido a la mayoría de casos que no se logra identificar al sujeto activo del delito teniendo como consecuencia el archivamiento definitivo de la investigación, quedando en impunidad el ilícito. Asimismo, se ha tratado de cambiar esa visión con la creación de fiscalías especializadas en delitos informáticos que tienen como finalidad de garantizar la lucha eficaz contra la ciberdelincuencia, pero esto resulta no suficiente porque se desconoce la gravedad de la problemática que se evidencia en las denuncias realizadas en la DIVINDAT y en nivel de fiscalía genera que no se logre la persecución en la sanción. Apreciándose la debilidad en la política del Estado para la prevención, detección y sanción de estos delitos, siendo que el sistema actual presenta estas particularidades que dificulta el accionar de prevenir, contrarrestar y sancionar los delitos informáticos, conllevando problemas ya que se puede desarrollar en cualquier parte del mundo y no se llega encontrar el lugar del ilícito, por lo que genera mayor complicación en la identificación y persecución, es por ello que debe utilizar aparatos legales internacionales con el propósito de

conseguir mayor eficacia en sanción del delito, por lo que Ministerio Público debe ofrecer un servicio eficiente, oportuno y especializado, es porque trata de lograr la Fiscalía Especializada en Delitos Informáticos es de perseguir de forma eficaz, implementando instrumentos tecnológicos de información y comunicación en mérito de poder detectar, identificar y perseguir con eficiencias esos comportamientos delictivos que se aprovechan de su conocimiento de informática.

VI. RECOMENDACIONES

PRIMERO: Que, el Congreso de la República del Perú, realice la modificatoria del artículo 8° de la Ley 30096, considerando que la finalidad de la norma es prevenir un acto delictivo y sancionar, para mantener el orden público. Dicho ello, se debe considerar expresamente la definición de delitos informáticos y delitos cibernéticos, para a partir de ello expresar las diversas modalidades que serían hechos de sanción, con la intención de evitar la vulneración de más víctimas de phishing y otras modalidades logrando alcanzar una tipificación concreta que permita al administrador de justicia emplear e interpretar coherentemente la ley.

SEGUNDO: Que, el Ministro del Interior ejecute y evalúe planos estratégicos de las modalidades de delitos informáticos más empleados; para de esta manera capacitar al personal de la DIVINDAT y fiscalías especializadas en esta materia; considerando políticas públicas como: presupuestos y medidas regulatorias institucionales que permitan la conexión de todas las entidades encargadas de investigar estos delitos informáticos en todas sus modalidades, permitiendo incluso la cooperación internacional de forma conjunta porque muchas veces el phisher se encuentra en otro país. Logrando criterios y avances concretos para un empleo eficaz de la normativa y una prevención del delito.

TERCERO: Que, los investigadores afines al estudio del fraude informático consideren generar conceptualizaciones y teorías legales sobre cada modalidad que va brotando con el avance de la tecnología, como en nuestro caso nos centramos en el phishing, el cual hemos podido investigar y observamos que se debe aclarar y precisar la norma; más cuando actualmente existe actividades ejecutadas en ciberespacio como por ejemplo el metaverso; temas colindantes a nuestra investigación.

REFERENCIAS

Abdulai, M, A. (2016). *Determinantes del miedo a la victimización del crimen de cibernética: un estudio del fraude a la tarjeta de crédito / débito entre estudiantes de la Universidad de Saskatchewan.* (Tesis de Maestría, Universidad de Saskatchewan). (Acceso el 15 de mayo de 2021).

Alarcon & Barrera (2017). *Uso de internet y delitos informáticos en los estudiantes de primer semestre de la Universidad Pedagógica y Tecnológica de Colombia, Sede Seccional Sogamoso 2016*. (Tesis de Grado, Universidad Norbert Wiener). Repositorio Institucional.

Alabdan,R.(2020).*Phishing Attacks Survey:Types, Vectors,and Techical Approaches.* https://doi.org/10.3390/fi12100168

Benito & Salinas (2016).*La investigación basada en el diseño en tecnología educativa.* http://dx.doi.org/10.6018/riite/2016/260631

Blossiers, J. (2003). *Criminalidad informática*. Lima: Editorial Portocarrero.

Cámara Nacional de Apelaciones en lo Criminal y Correccional. Sala V. (agosto 2016). https://jurisprudencia.mpd.gov.ar/Boletines/2016.08.%20Delitos%20informaticos.pdf

Chaparro, M. F. (2014). *Legislación informática y protección de datos en Colombia, comparada con otros países*. INVENTUM, 9(17), 32-37. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=&ved=2ahUKEwiSlKXsv67xAhWOHLkGHdDND1kQFjABegQIBBAE&url=https%3A

%2F%2Frevistas.uniminuto.edu%2Findex.php%2FInventum%2Farticle%2Fdownload%2F1014%2F953%2F&usg=AOvVaw2oDJcLmoStyRda3ALW220x

Chilcon (2019). *EL CIBERCRIMEN EN EL PERU Y SU INCIDENCIA EN LA SEGURIDAD NACIONAL*. (Tesis de Grado, Centro de Altos Estudios Nacionales). Repositorio Institucional. https://core.ac.uk/reader/201883803

Código Penal Alemán. (2002, 30 de agosto). https://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20080616_02.pdf

Congreso de la Republica. (2013, 21 de octubre). Ley Nª 30096.Ley de Delitos Informáticos. https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096

Consejo General del Poder Judicial de Logroño de España (2014,16 de abril). Sentencia 77/2014 (Maria del Puy Aramendia Ojer). https://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7095915&links="phishing"&optimize=20140613&publicinterface=true

Convención de Budapest contra la ciberdelincuencia. (2021, 23 de noviembre). https://www.oas.org/juridico/english/cyb_pry_convenio.pdf

Dumisani,G.(2018). '*Understanding the threat of cybercrime: A comparative study of cybercrime and the ICT legislative frameworks of South Africa, Kenya, India, the United States and the United Kingdom'. https://open.uct.ac.za/bitstream/handle/11427/29247/thesis_law_2018_gumbi_dumisani.pdf?sequence=1&isAllowed=y*

Erazo,M (2011).*Rigor científico en las prácticas de investigación cualitativa.* https://www.redalyc.org/pdf/145/14518444004.pdf

Espinoza (2017). *DERECHO PENAL INFORMÁTICO: DESLEGITIMACIÓN DEL PODER PUNITIVO EN LA SOCIEDAD DE CONTROL*. (Tesis de Grado, Universidad Nacional del Altiplano). Repositorio Institucional. http://repositorio.unap.edu.pe/bitstream/handle/UNAP/6309/Espinoza_Coila_Michael.pdf?sequence=1&isAllowed=y

Fadare,O & Zahurin, M. (2021).*Fight Against Phishing Attacks Amang Internet Banking User: A knwledge Management Technique.* *http://www.kmice.cms.net.my/ProcKMICe/KMICe2021/pdf/CR205.pdf*

Fatima, R., Yasin, A., Liu, L., & Wang, J. (2019). How persuasive is a phishing email? A phishing game for phishing awareness. *Journal of Computer Security, 27*(6), 581-612. http://dx.doi.org/10.3233/JCS-181253

Fernández, L., Cabezudo, J., Arenas, M., Herrera, R., & Gastelu, J. (2010). *Diseño de herramientas de control y medidas de prevención para evitar ser víctimas de Delitos Informáticos*. Fernández, L, Cabezudo, J. Arenas , M. Herrera, R. Gastelu, J. Perú: Policía Nacional del Perú. http://www.buenastareas.com/ensayos/Dise%C3%B1o-De-Herramientas-DeControl-Inform%C3%A1tico/1245461.html

Fiscalía de la Nación. (2020, 30 de noviembre). Crean la Unidad Fiscal Especializada. Diario Oficial el peruano. https://busquedas.elperuano.pe/normaslegales/crean-la-unidad-fiscal-especializada-en-ciberdelincuencia-de-resolucion-no-1503-2020-mp-fn-1916745-1/

Flores, Mosquera y los miembros del Consejo Nacional de Política Criminal (2020).Diagnóstico situacional multisectorial sobre la ciberdelincuencia en el Perú. https://cdn.www.gob.pe/uploads/document/file/1487798/01%20Diagnóstico%20Situacional%20Multisectorial%20sobre%20la%20Ciberdelincuencia%20en%20el%20Perú%20%281%29.pdf.pdf

Habirovs, Arturs.(2018).*Factors thay shape cybercrime civtimisation and use of prevention measures in Englad and Wales.* *http://eprints.hud.ac.uk/id/eprint/35042/1/FINAL%20THESIS%20-%20HABIROVS.pdf*

Hernandez, Fernández, & Baptista (2014). *Metodología de la investigación.* 6.ª ed. México: McGraw-Hill/ Interamericana Editores, S.A. DE C.V. https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Herrera, C, E. (2016). "*El Phishing como Delito Informático y su Falta de Tipificación en el Código Orgánico Integral Penal".* (Tesis de Grado, Universidad Central de Ecuador). Repositorio Institucional. http://www.dspace.uce.edu.ec/bitstream/25000/8132/1/T-UCE-0013-Ab-399.pdf

Hidalgo (2018). *"Los delitos informáticos y su afectación sobre los bienes jurídicos"*. (Tesis de Grado, Universidad Católica de Santiago de Guayaquil). Repositorio Institucional. http://repositorio.ucsg.edu.ec/bitstream/3317/10643/1/T-UCSG-PRE-JUR-DER-MD-196.pdf

Jefatura del Estado. (23 de noviembre de 1995). Ley Orgánica 10/1995. Código Penal Español. https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf

Junger, M, Abhishta,A & Nieuwenhuis,B.(2018*). Crime chain: het verband tussen DDoS-aanvallen en Phishing. https://www.researchgate.net/publication/352903865_Crime_chain_het_verband_tussen_DDoS-aanvallen_en_Phishing*

Kasem Bundit University. (2018). *Legal Limitations relating to the Application of Thai Computer – related Crime Act of B.E. 2560 to the case of "Phishing.* https://so04.tci-thaijo.org/index.php/jkbu/article/view/130226/99100

Lamperti, S. B. (2017). *Aspectos Legales. Los Delitos Informáticos. El rastro digital del delito: aspectos técnicos, legales y estratégicos de la Informática Forense*. Mar de Plata: Universidad FASTA Ediciones.Recuperado de: http://redi.ufasta.edu.ar:8080/xmlui/handle/123456789/1593

Landa, C., & Velazco, A. (2007). *Constitución Política del Perú*. Lima: Fondo Editorial de la Pontificia Universidad Católica del Perú.

Leukfeldt, E. R. (2014). Cybercrime and social ties: Phishing in amsterdam. *Trends in Organized Crime, 17*(4), 231-249. http://dx.doi.org/10.1007/s12117-014-9229-5

Mariana, M. (2015).*EL PHISHING.* (Tesis de Grado,Universitat Jaume-I). Repositorio Institucional.

http://repositori.uji.es/xmlui/bitstream/handle/10234/127507/TFG_Leguizamón_Mayra.pdf?sequence=1

Matusan, C. (2013). *La Acción Penal Privada y la afectación de derechos fundamentales.* Revista VIA IURIS, (14),187-197. ISSN: 1909-5759. https://www.redalyc.org/pdf/2739/273929754011.pdf

Ministerio de Justicia. Derechos Humanos y Cultos.Subsecretaria de desarrollo normativo. (2014, 10 de febrero). Código Orgánico Integral Penal. https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_con_judi_cód_org_int_pen.pdf

Ministerio de Justicia. Ley no. 19.223. (1993,07 de junio). https://derecho.udd.cl/actualidad-juridica/files/2021/01/AJ29_553.pdf

Ministerio Público – Fiscalía Superior Especializada en Delitos de Ciberdelincuencia de Lima. (2021, 17 de junio). Detienen a integrante de banda en primer caso de delito informático con investigación fiscal especializada. [página de Facebook]. Facebook. https://www.facebook.com/FiscaliaPeru/posts/4034512379964204

Morales, F. (2012, 19 de septiembre). Con*ozca 3 tipos de investigación: Descriptiva, Exploratoria y Explicativa. Creades*. https://bit.ly/31rIhJm

Muntode,A., Parwe,S. (2019). An Overview on Phishing-its types and Countermeasures. https://pdfs.semanticscholar.org/6940/19bc2e2fdea1f62975fa80915befb48cfb28.pdf

Nessi, A. (2017). Manual de evidencia digital.Recuperado de: https://www.mpfn.gob.pe/Docs/0/files/manual_evidencia_digital.pdf

Nishad,M. (2018).*A Review Paper on Phishing Through E-Mail*. https://www.neliti.com/publications/263164/a-review-paper-on-phishing-through-e-mail

Oficina de Analisis Estrategico contra la Criminalidad.(febrero 2021).Informe de Analisis Nº 4 *Ciberdelincuencia:Pautas para una investigación fiscal especializada.*

https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERÚ%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIÓN%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf

Pardo (2018). *Tratamiento juridico penal de los delitos informaticos contra el patrimonio , Distrito Judicial de Lima , 2018*.(Tesis de Grado, Universidad Cesar Vallejo).Repositorio Institucional. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y

Pons (2018*). "Ciberterrorismo: Amenaza a la seguridad. Respuesta operativa y legislativa, nacional e internacional"*. (Tesis Doctoral, Escuela Internacional de Doctorado). Repositorio Institucional. http://e-spacio.uned.es/fez/eserv/tesisuned:ED-Pg-DeryCSoc-Vpons/PONS_GAMON__Vicente_Tesis.pdf

Quintana, A. (2006). *Metodología de investigación científica cualitativa*. En Quintana Peña, A. y Montgomery, W. (Eds.) Psicología tópicos de actualidad, 65-73. Lima:UNMSM. http://biblioteca.udgvirtual.udg.mx/jspui/handle/123456789/2724

Ramírez, D. A., y Castro, E. F. (2018). *Análisis de la evidencia digital en Colombia como soporte judicial de delitos informáticos mediante cadena de custodia.* Villavicencio: Universidad Nacional Abierta y a Distancia "UNAD". https://repository.unad.edu.co/bitstream/handle/10596/17370/86078250.pdf?sequence=1&isAllowed=y

Reyes (2020). *Los delitos informaticos y su influencia en Integridad Personal, distrito de Chorrillos, Lima Metropolitana, 2019*. (Tesis de Grado, Universidad Peruana de las Américas). Repositorio Institucional. http://repositorio.ulasamericas.edu.pe/bitstream/handle/upa/937/T.%20INVESTIGACION-REYES%20VALDIVIA.pdf?sequence=1&isAllowed=y

Rodríguez, F. (2013). *Derecho informático. El derecho en la era digital. La sociedad de información y el sistema jurídico. Contratos informáticos. Protección jurídica de los programas de computación. Delitos informáticos. La tutela*

jurídica del sistema informático. UNC y FCEFyN. http://www.feliperodriguez.com.ar/wp-content/uploads/2013/11/LIBRO-7-DERECHO-INFORMATICO.pdf

Sanchez (2017). *"ADOPCIÓN DE ESTRATEGIAS DE CIBERSEGURIDAD EN LA PROTECCIÓN DE LA INFORMACIÓN EN LA OFICINA DE ECONOMÍA DEL EJÉRCITO, SAN BORJA- 2017"*. (Tesis de Grado, Instituto Tecnológico del Ejército). Repositorio Institucional. http://repositorio.icte.ejercito.mil.pe/bitstream/ICTE/26/1/Tesis%20John%20Sanchez%20Blas.pdf

Sánchez, J. (2009). *El bien jurídico protegido en el delito de estafa informática*.Recuperado de: https://dialnet.unirioja.es/servlet/articulo?codigo=3760666

Santoso, J y Nasution,M.(2021). *Analysis of Community Awareness Against Threats to Personal Data Security Through Phishing Websites.* http://www.stmik-budidarma.ac.id/ejurnal/index.php/ijics/article/view/3053

Shakthidhar,G,Jayati,D,Marthie,G,Donglnn,K ,Sanchari,D & L,J.(2021).*Cross-National Study on Phishing Resilience. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3859057*

Valderrama, S .*Pasos para elaborar proyectos y tesis de investigación científica.* San Marcos; Lima.

V Bhavsar, A Kadlak, S Sharma - Int. J.(2018). *Study on Phishing Attacks.* https://www.researchgate.net/profile/Shabnam-Sharma-2/publication/329716781_Study_on_Phishing_Attacks/links/5ef9867a92851c52d6069bf2/Study-on-Phishing-Attacks.pdf

Yatsyk,T y Shkelebei,V.(2018). *INVESTIGATION OF NEW FORMS OF CYBER CRIME (PHISHING AND CYBERSQUATTING).* https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/30706/1/INVESTIGATION%20OF%20NEW%20FORMS%20OF%20CYBER%20CRIME.pdf

Yue Ba.(2017).*UNDERSTANDING CYBERCRIME AND DEVELOPING A MONITORING DEVICE.*

https://www.theseus.fi/bitstream/handle/10024/132641/Ba_Yue.pdf?sequence=1&isAllowed=y

Zorrilla (2018). INCONSISTENCIAS Y AMBIGÜEDADES EN LA LEY DE DELITOS INFORMÁTICOS LEY Nº 30096 Y SU MODIFICATORIA LEY Nº 30171. (Tesis de Grado, Universidad Nacional de Ancash “Santiago Antunez de Mayolo”). Repositorio Institucional. http://repositorio.unasam.edu.pe/bitstream/handle/UNASAM/2332/T033_70221905_T.pdf?sequence=1&isAllowed=y

ANEXO 03

MATRIZ DE CATEGORIZACIÓN APRIORÍSTICA

NOMBRE DE LAS ESTUDIANTES: Zavala Alzamora, Karolein Mishel Magdelein

Vigo Baca, Luz Benilda

FACULTAD DE DERECHOS Y HUMANIDADES

ESCUELA: Escuela Profesional de Derecho

ÁMBITO TEMÁTICO: De la estructura del estado y Delitos contra el patrimonio

TÍTULO	
Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020	
PROBLEMAS	
Problema General	¿Qué efectos genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020?
Problema Específico 1	¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa?
Problema Específico 2	¿Cómo enfrentó el Ministerio Público la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras?
OBJETIVOS	
Objetivo General	Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.
Objetivo Específico 1	Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa.
Objetivo Específico 2	Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras.
SUPUESTOS	
Supuesto General	La ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima; generó como principales efectos, la falta de seguridad informática y daños patrimoniales; porque el usuario, consumidor o también denominado víctima, se encontró con discrepancias en el tratamiento de las leyes penales.
Supuesto Específico 1	La protección a las víctimas de phishing en entidades financieras, se vulneró al no respetar el derecho de estas personas y por el mal actuar de los administradores de justicia; lo cual, fue evidenciado con las denuncias.

Supuesto Específico 2	El Ministerio Público enfrentó la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras de una manera concreta y productiva; por ello, formó la Unidad Fiscal Especializada en Ciberdelincuencia, porque se observó el incremento de ciberdelitos en la modalidad phishing en la época de pandemia, sin embargo eso no fue suficiente.
Categorización	**Categoría 1: Ineficacia Normativa** Subcategorías 1: Marco legal. Subcategorías 2: Modalidades frecuentes en delitos informáticos. **Categoría 2: Víctimas De Phishing** Subcategorías 1: Categorización de víctimas. Subcategorías 2: Actuación del Ministerio Público.
MÉTODO	
Tipos, diseño y nivel de investigación	**Enfoque:** Cualitativo **Diseño:** Teoría Fundamentada **Tipo de investigación**: Básica **Nivel de la investigación:** Descriptivo
Muestreo	**Escenario de estudio:** Fiscalía penal, despachos judiciales penales, estudios jurídicos, división de investigación de delitos de alta tecnología. **Participantes:** Dos jueces (Corte Superior de Justicia de Lima Sur y Lima Norte), un Fiscal Adjunto Provincial Penal(Ministerio Público de Lima Norte), un comandante de la Policía Nacional del Perú (Mayor – Ex jefe del equipo de investigaciones de la DIVINDAT), un Ex director contra el crimen organizado (Ministerio del interior) y tres abogados penalistas. **Muestra:** No probabilística. **Muestra No probabilística – Tipo**: De experto. **Muestra orientada:** Por conveniencia.
Técnica e instrumento de recolección de datos	**Técnica:** Entrevista y análisis de documentos. **Instrumento:** Guía de entrevista y ficha de análisis de fuente documental: Jurisprudencia internacional, derecho comparado, informe de análisis estratégico, artículo informativo en página web, resolución de la Fiscalía de la Nación.
Método de análisis de datos	Análisis hermenéutico, descriptivo e inductivo.

ANEXO 04: INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

Titulo: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Entrevistado/a:
Cargo/profesión/grado académico:
Normas básicas de la entrevista:

I. INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responde desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: La protección a las víctimas de phishing hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, categorizados mayormente de forma errónea con la figura de “estafas”; por ello, que las entidades financieras buscan protegerse y también al usuario o consumidor a través de las normas establecidas; por tanto.

01.- Desde su experiencia profesional, diga Ud., ¿De qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?

……

02- El fraude informático es la vulneración del conjunto de reglas normativas sobre informática referente a todas sus manifestaciones. El artículo N°8 de la Ley N°30096 – Ley de Delitos Informáticos, señala en su primer párrafo al sujeto activo indicando las acciones ilícitas que serán reprimidas con una pena privativa de libertad o días multa; según su criterio, ¿Considera que la regulación vigente es eficiente para contrarrestar en los delitos de phishing?

……..……
……..……

03.- De acuerdo al Convenio de Budapest, el fraude informático está denominado como actos deliberados e ilegítimos que ocasionan perjuicio patrimonial a otro individuo, ¿Considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?

……
……

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa.

Premisa: Las entidades financieras se han adecuado a un proceso de globalización que conlleva a generar enormes cambios para la sociedad en consecuencia de los diversos delitos de la tecnología que infringen a la estabilidad y protección a nivel internacional; tanto de las personas jurídicas como naturales, presentándose bajo diferentes modalidades de sistemas o redes informáticas, generando una complejidad operativa y cambios constantes que dificultan su persecución.

04.- Según su punto de vista, ¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, Lima 2020?

……
……
……
……
……

05.- La víctima de phishing es el sujeto pasivo, ignorante en tecnología y por ello es más vulnerable en los delitos cibernéticos; los cuales, se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica.

Dentro de su perspectiva, ¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?

……
……

06.- Según sus erudiciones legales, ¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MPFN?.

……
……
……
……..

Objetivo específico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras.

Premisa: Todo operador de justicia debe aprender el manejo de equipos actualizados ante la modernización de la delincuencia. El Ministerio Público tiene como meta orientar técnica y legalmente en las investigaciones de delitos informáticos, coordinando en todo el país con organismos estatales y privados.

07.- Explique ¿De qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?

……
……
……

……

08.- ¿Qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?

……
……
……
……

……
……

09.- Una medida propuesta es la difusión de información por parte de las autoridades estatales y privadas a fin de propiciar la prevención del delito informático de Phishing, ¿Considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?

……
……
……
……
……
……

Entrevistador: **DNI:**	**Entrevistado:** **DNI:**

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 5

VALIDACION DE INSTRUMENTO

I.- DATOS GENERALES

1.1. Apellidos y Nombres: Dr. Santisteban Llontop, Pedro
1.2. Cargo e institución donde labora: Docente UCV.
1.3. Nombre del instrumento motivo de evaluación: **Guía de Entrevista.**
1.4. Autor de Instrumento: Zavala Alzamora Karolein Mishel Magdelein
Vigo Baca Luz Benilda

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	No cumple con su aplicación						Cumple en parte con su aplicación			Si cumple consu aplicación			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguajeapropiado.												X	
2. OBJETIVIDAD	Se expresar la realidad como es, indica cualidad de objetivo y laadecuación al objeto investigado												X	
3. ACTUALIDAD	Esta de acorde a los aportes recientes al derecho.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Cumple con los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las Categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentostécnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos y supuestos, basado en los aspectos teóricos y Científicos												X	
9. METODOLOGÍA	El instrumento responde al objetivo de la Investigación: Tipo, diseño, categorías, escenario de estudios y participantes.												X	
10. PERTINENCIA	El instrumento tiene sentido, enfrenta un problema crucial, está situado en una población en territorio,es interdisciplinaria, tiene relevancia global, y asume responsablemente las consecuencias de sus hallazgos.												X	

II. OPINIÓN DE APLICABILIDAD

El Instrumento cumple con los Requisitos para su aplicación	**SI**
El Instrumento cumple en parte con los Requisitos para su aplicación	
El Instrumento no cumple con los requisitos para su aplicación	

III. PROMEDIO DE VALORACIÓN:

95 %

Lima, 30 de Setiembre 2021.

FIRMA DEL EXPERTO INFORMANTE
Pedro Santisteban Llontop
DNI N° 09803311 Tel 983278657

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 06

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Wenzel Miranda Eliseo Segundo.
1.2. Cargo e institución donde labora: Docente UCV.
1.3. Nombre del instrumento motivo de evaluación: GUIA DE ENTREVISTA.
1.4. Autor(A) de Instrumento: Zavala Alzamora Karolein Mishel Magdelein
Vigo Baca Luz Benilda

II. ASPECTOS DE VALIDACIÓN

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

III. OPINIÓN DE APLICABILIDAD

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

IV. PROMEDIO DE VALORACIÓN:

95%

Lima, 24 de Junio del 2021.

FIRMA DEL EXPERTO INFORMANTE
DNI N° 09940210 Telf. 992303480

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 5

VALIDACION DE INSTRUMENTO

I.- DATOS GENERALES

1.1. Apellidos y Nombres: Luca Aceto
1.2. Cargo e institución donde labora: Docente UCV.
1.3. Nombre del instrumento motivo de evaluación: **Guía de Entrevista.**
1.4. Autor de Instrumento: Zavala Alzamora Karolein Mishel Magdelein
Vigo Baca Luz Benilda

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	No cumple con suaplicación						Cumple en parte con su aplicación			Si cumple con su aplicación			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje apropiado.												X	
2. OBJETIVIDAD	Se expresar la realidad como es, indica cualidad de objetivo y la adecuación al objeto investigado												X	
3. ACTUALIDAD	Esta de acorde a los aportes recientes al derecho.												X	
4. ORGANIZACIÓN	Existe una organización lógica.												X	
5. SUFICIENCIA	Cumple con los aspectos metodológicos esenciales												X	
6. INTENCIONALIDAD	Esta adecuado para valorar las Categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentostécnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos y supuestos, basado en los aspectos teóricos y Científicos												X	
9. METODOLOGÍA	El instrumento responde al objetivo de la Investigación: Tipo, diseño, categorías, escenario de estudios y participantes.												X	
10. PERTINENCIA	El instrumento tiene sentido, enfrenta un problema crucial, está situado en una población en territorio, es interdisciplinaria, tiene relevancia global, y asume responsablemente las consecuencias de sus hallazgos.												X	

IV. OPINIÓN DE APLICABILIDAD

El Instrumento cumple con los Requisitospara su aplicación	**SI**
El Instrumento cumple en parte con losRequisitos para su aplicación	
El Instrumento no cumple con los requisitos para su aplicación	

V. PROMEDIO DE VALORACIÓN:

95 %

Lima, 30 de Setiembre 2021.

FIRMA DEL EXPERTO INFORMANTE
Luca Aceto
DNI N° 48974953

ANEXO 04: INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

Titulo: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Entrevistado/a: Lenin Aldo Segundo Ayala
Cargo/profesión/grado académico: Juez Especializado Penal
Normas básicas de la entrevista:

I. **INSTRUCCIONES:**

Leer detenidamente cada interrogante de la presente entrevista y responde desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: La protección a las víctimas de phishing hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, categorizados mayormente de forma errónea con la figura de "estafas"; por ello, que las entidades financieras buscan protegerse y también al usuario o consumidor a través de las normas establecidas; por tanto.

01.- Desde su experiencia profesional, diga Ud., ¿De qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?

La ineficacia normativa resalta al no haber una legislación que proteja a la víctima del phishing, pues las entidades bancarias e INDECOPI, determinan responsabilidad en el cliente. Además, existe una disyuntiva si el phishing es un delito informático o una estafa por qué el fin es el hurto del dinero que se encuentra en la cuenta de ahorros o en la tarjeta de crédito; sin tomar en cuenta el medio por el cual se realiza dicha acción.

02- El fraude informático es la vulneración del conjunto de reglas normativas sobre informática referente a todas sus manifestaciones. El artículo N°8 de la Ley N°30096 – Ley de Delitos Informáticos, señala en su primer párrafo al sujeto activo indicando las acciones ilícitas que serán reprimidas con una pena privativa de libertad o días multa; según su criterio, ¿Considera que la regulación vigente es eficiente para contrarrestar los delitos informáticos en la modalidad de phishing?

No, porque el phishing es cometido por organizaciones criminales bien organizadas; además la regulación no es precisa y no indica las modalidades; por ello, estas organizaciones ilícitas crecen en su logística y generan un peligro latente cada vez más grande. Debiéndose regularizar la norma para que las entidades bancarias faciliten las informaciones de manera rápida solo con la fragancia del delito o con una disposición fiscal para luego confirmar esta disposición por el juzgado respectivo.

03.- De acuerdo al Convenio de Budapest, el fraude informático está denominado como actos deliberados e ilegítimos que ocasionan perjuicio patrimonial a otro individuo, ¿Considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?

Sí, las leyes impuestas son semejantes a la legislación existente en el convenio; porque al ser parte tiene una legislación homogénea entre los demás paises miembros, pero esto no se ajusta a la realidad, además que hace falta políticas públicas.

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa.

Premisa: Las entidades financieras se han adecuado a un proceso de globalización que conlleva a generar enormes cambios para la sociedad en consecuencia de los diversos delitos de la tecnología que infringen a la estabilidad y protección a nivel internacional; tanto de las personas jurídicas como naturales, presentándose bajo

diferentes modalidades de sistemas o redes informáticas, generando una complejidad operativa y cambios constantes que dificultan su persecución.

04.- Según su punto de vista, ¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa?

Se vulneran a estas víctimas con la falta de ejercer bien la administración de justicia, ya que no se encuentra la responsabilidad en quien ejecuta dichos actos, sino todo lo contrario, el cliente de la entidad bancaria sale perjudicado y no existen muchos especialistas en estos temas que lo puedan asesorar.

05.- La víctima de phishing es el sujeto pasivo, ignorante en tecnología y por ello es más vulnerable en los delitos cibernéticos; los cuales, se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica.

Dentro de su perspectiva, ¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?

Si, porque esto permitiría identificar al autor del acto delictivo conforme a la manera de escoger a sus víctimas. Incluso, los datos de cifras actualizadas y categorizadas llevarían a ver el margen de crecimiento y los formas de contrarrestar estas modalidades.

06.- Según sus erudiciones legales, ¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MPFN?

Si, deben hacerse cambios en la legislación y especificar las modalidades, para permitir la identificación adecuada del autor y una acusación del hecho punible acorde a la norma. De esta manera, la personas que son víctimas de phishing, estarían más protegidas ante la actuación de los administradores de justicia que muchas veces cometen errores en la imputación del delito.

Objetivo específico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras.

Premisa: Todo operador de justicia debe aprender el manejo de equipos actualizados ante la modernización de la delincuencia. El Ministerio Público tiene como meta orientar técnica y legalmente en las investigaciones de delitos informáticos, coordinando en todo el país con organismos estatales y privados.

07.- Explique ¿De qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?

La actuación del Ministerio Pública se ha visto en la creación de la Nueva Fiscalía Especializada en Ciberdelitos; sin embargo, falta la capacitación del personal para poder interpretar la norma y aportar ayuda a las víctimas de estos delitos. Además, a ello se suma que esta fiscalía no es suficiente para todo el país.

08.- ¿Qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?

La implementación de despachos fiscales sería una actuación muy eficiente, si se suma con ello las capacitaciones y un presupuesto adecuado para que se mantengan actualizados tanto el aporte humano como el material. También, es preciso requerir de peritos informáticos, los cuales permitirían una identificación del autor (pisher) para la respectiva individualización, evitando con ello el archivo de tantos casos referentes de los delitos cibernéticos.

09.- Una medida propuesta es la difusión de información por parte de las autoridades estatales y privadas a fin de propiciar la prevención del delito informático de Phishing, ¿Considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?

Si, la educación y la prevención que se debe generalizar en los clientes bancarios y los administradores de justicia, tanto policías como fiscales y jueces; para evitar más víctimas de fraudes informáticos. Teniendo en cuenta que esta responsabilidad de educación no solo recae en el estado, también debe tener participación de las entidades bancarias quienes deberían de preocuparse por la falta de conocimiento de sus clientes ante estos hechos delictivos.

Firma:

Entrevistado: Lenin Aldo Segundo Ayala

DNI:44515819

ANEXO 04: INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

Titulo: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Entrevistado/a: Jose Luis Borda Rubatto
Cargo/profesión/grado académico: Fiscal Adjunto Provincial Penal
Normas básicas de la entrevista:

I. INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responde desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: La protección a las víctimas de phishing hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, categorizados mayormente de forma errónea con la figura de "estafas"; por ello, que las entidades financieras buscan protegerse y también al usuario o consumidor a través de las normas establecidas; por tanto.

01.- Desde su experiencia profesional, diga Ud., ¿De qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?

Que, dado el estado de emergencia que la nación ha sufrido ha hecho que los ciudadanos realicen y efectúen un mayor uso de la tecnología para la adquisición de bienes y servicios, muchas veces de ellos las entidades prestadoras de estos servicios solicitaban que las transferencias se efectuaran mediante la modalidad en línea, por ejemplo la compra de víveres de Wong, mi banda y etc., entonces se ha realizado, empero muchas veces ha pasado que las paginas web fueron clonadas, con el fin de vulnerar el servicio y la legislación tiene un vacío, dado que existe una afectación al consumir, lo cual ha procedido con las denuncias de fraude informático y las entidades financieras y de servicios no han podido solucionar esta situación, puesto que no existe legislación alguna que en cierta medida haya podido resolver este conflicto de intereses

02- El fraude informático es la vulneración del conjunto de reglas normativas sobre informática referente a todas sus manifestaciones. El artículo N°8 de la Ley N°30096 – Ley de Delitos Informáticos, señala en su primer párrafo al sujeto activo indicando las acciones ilícitas que serán reprimidas con una pena privativa de libertad o días multa; según su criterio, ¿Considera que la regulación vigente es eficiente para contrarrestar los delitos informáticos en la modalidad de phishing?

Según la legislación contempla que el sujeto activo utiliza un medio tecnológico para realizar estafar financieras a personas que aceden a dichos servicios para la satisfacción de una necesidad al encontrarse un vacío normativo en la identificación del sujeto pasivo trae consigo una deficiencia de identificación del sujeto que ha efectuado el delito informático, por lo que existe un vacío legal, a su vez tampoco existe una normatividad administrativa que regule de manera técnica la búsqueda e identificación del autor material que ha cometido el ilícito penal del delito informático.

03.- De acuerdo al Convenio de Budapest, el fraude informático está denominado como actos deliberados e ilegítimos que ocasionan perjuicio patrimonial a otro individuo, ¿Considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?

De que se necesita una mayor precisión sobre le identificación del sujeto activo que comité el ilícito penal.

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa.

Premisa: Las entidades financieras se han adecuado a un proceso de globalización que conlleva a generar enormes cambios para la sociedad en consecuencia de los diversos delitos de la tecnología que infringen a la estabilidad y protección a nivel internacional; tanto de las personas jurídicas como naturales, presentándose bajo diferentes modalidades de sistemas o redes informáticas, generando una complejidad operativa y cambios constantes que dificultan su persecución.

04.- Según su punto de vista, ¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa?

……

……

……

……

……

05.- La víctima de phishing es el sujeto pasivo, ignorante en tecnología y por ello es más vulnerable en los delitos cibernéticos; los cuales, se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica.

Dentro de su perspectiva, ¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?

Que si, es necesario categorizarlo dado que los delitos informáticos pueden abarcar lesiones contra el patrimonio, libertad sexual y otro.

06.- Según sus erudiciones legales, ¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MPFN?

Que si consideramos necesario, que en la Ley se tiene que implementar pero normas de carácter de la especialización y que coayudan a una mejor investigación del ministerio Publico.

Objetivo específico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras.

Premisa: Todo operador de justicia debe aprender el manejo de equipos actualizados ante la modernización de la delincuencia. El Ministerio Público tiene como meta orientar técnica y legalmente en las investigaciones de delitos informáticos, coordinando en todo el país con organismos estatales y privados.

07.- Explique ¿De qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?

El Ministerio Publico dentro de sus funciones está la de investigar un hecho delictuoso aplicando lo establecido en el Código Penal y su Ley orgánica, para la identificación de víctimas de phishing en entidades financieras se hace necesario la presentación de un proyecto de ley que la misma que puede ser por la máxima de la experiencia por los casos que se vienen investigando, donde se evidencias las falacias normativas y ser más eficaces para la resolución del delito.

08.- ¿Qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?

Que conforme se tiene de la disposición de la Fiscal de la Nación se han creado las fiscalías especializadas en delitos informáticos, empero se ha entendido que dichas

solo emiten opiniones para la investigación las mismas que son realizadas por las fiscalías comunes, a su vez se tiene que tomar en cuenta de la gran cantidad de hecho punibles cometidos por los sujetos activo del delito informático, estos casos se han incrementado, por lo que debería de darse el verdadero significado y especialización a dichas fiscalías dado que son los únicos que podrían investigar los delitos informático.

09.- Una medida propuesta es la difusión de información por parte de las autoridades estatales y privadas a fin de propiciar la prevención del delito informático de Phishing, ¿Considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?

Que, si estamos de acuerdo que el estado pueda difundir sobre los alcances del delito informático, pero a su vez se hace necesario que las entidades financieras también realicen y/o proponen la protección de datos para el uso de los servicios de internet.

Firma:

Entrevistado: Jose Luis Borda Rubatto

DNI: 41615316

ANEXO 04: INSTRUMENTO DE RECOLECCIÒN DE DATOS

GUIA DE ENTREVISTA

Titulo: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Entrevistado/a: Juan Antonio Pozo Castillo
Cargo/profesión/grado académico: Ex mayor jefe de equipo de investigaciones / comandante de la Policía Nacional del Perú

Normas básicas de la entrevista:

I. INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responde desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: La protección a las víctimas de phishing hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, categorizados mayormente de forma errónea con la figura de "estafas"; por ello, que las entidades financieras buscan protegerse y también al usuario o consumidor a través de las normas establecidas; por tanto.

01.- Desde su experiencia profesional, diga Ud., ¿De qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?

El Phisging, como modalidad delictiva no está tipificada en la Ley de Delitos Informáticos N° 30096, se comete a través del internet mediante el uso de ingeniería social, es un virus que es enviado por los ciberdelincuentes en forma masiva con una página falsa de una entidad bancaria donde generalmente indican que actualice sus datos o se ha hecho acreedor a una promoción al hacer clic en este vínculo lo re direcciona a otra página falsa de banco y le capta los datos confidenciales de su tarjetas electrónicas bancarias, ahora bien la entidad bancaria es la responsable que su cliente haya ingresado sus datos confidenciales en un página falsa y le hayan captado estos datos para posteriormente ser usados en forma inmediata por realizar transferencias ilícitas de dinero o realizar compras por internet, en este caso el cliente es el responsable ya que no tiene instalado un antivirus actualizado con la licencia vigente, o por haber ingresado a la página del banco en forma no segura por intermedio de algún motor de búsqueda (Google u otros).

Ante esta situación estamos en una disyuntiva si el phishing es un delito informático o una estafa por qué el fin es el hurto del dinero que se encuentra en la cuenta de ahorros o en la tarjeta de crédito.

Por tal motivo no hay una legislación que proteja a la víctima del phisging, ya que las entidades bancarias y muchas veces INDECOPI, determina responsabilidad en el cliente.

Pero las entidades bancarias tienen la obligación de:

a) Realizar la ciberseguridad de sus sitios web que se encuentran en el ciberespacio para proteger a sus clientes de las diferentes clases de virus y malware como son el pharming, phishing o defacement, que son elaborados muy técnicamente por ciberdelincuentes a nivel mundial.
b) Detectar, neutralizar y eliminar en los motores de búsqueda (Google y otros) los sitios web con indicación BBVA, con la finalidad de evitar que sus clientes entren a páginas clonadas y sean víctimas de fraudes informáticos con el uso de la información reservada de sus cuentas o tarjetas de créditos.
c) El Banco tiene conocimiento que sus miles de clientes todos no tienen conocimientos básicos de informática, o el uso de la tecnología aplicada a los teléfonos celulares asimismo tiene clientes de todas las edades desde muy jóvenes hasta adultos mayores y estos últimos son muy susceptibles de ser víctimas de actos delincuenciales en agravio de su patrimonio bajo el cuidado y administración del banco.

02- El fraude informático es la vulneración del conjunto de reglas normativas sobre informática referente a todas sus manifestaciones. El artículo N°8 de la Ley N°30096 – Ley de Delitos Informáticos, señala en su primer párrafo al sujeto activo indicando las acciones ilícitas que serán reprimidas con una pena privativa de libertad o días

multa; según su criterio, ¿Considera que la regulación vigente es eficiente para contrarrestar los delitos informáticos en la modalidad de phishing?

No es para nada eficiente ya que el phishing, es comedido por organizaciones Criminales muy bien constituidas y organizadas y cada uno tiene un rol definido desde el CRAKER que envía el virus, otros miembros se encargan de la parte logística, inmuebles maquinas computadoras conseguir internet, otro delincuente se encarga de captar a las cuentas receptoras o beneficiarias denominadas MULAS, otro se encarga de recibir y administrar el dinero y finalmente la cuenta receptora o mula quien es la encargada de proporcionar su tarjeta electrónica bancaria para el retiro de dinero y si es una cantidad fuerte este sujeto se persona a la ventanilla del banco y retira el dinero que posterior es entregado al miembro de la organización criminal.

Ante estas circunstancias la pena debe ser más drástica y debe ser investigado por organizaciones criminales o bandas criminales, asimismo se debe regularizar la legislación para que las entidades bancarias proporcionen las informaciones en forma inmediata solo con la fragancia del delito o con una disposición fiscal para después convalidar esta disposición por el juzgado respectivo, teniendo en cuenta que es muy importante capturar a la cuenta receptora en fragancia para que de esta manera identificar a los demás miembros de la organización o banda criminal, generalmente se identifica a la cuenta receptora más a los otros delincuentes.

03.- De acuerdo al Convenio de Budapest, el fraude informático está denominado como actos deliberados e ilegítimos que ocasionan perjuicio patrimonial a otro individuo, ¿Considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?

Si la Ley 30096 y su modificatoria Ley 30771, son idénticas a la legislación existente en el convenio de Budapest y esto tiene una razón de ser ya que un país sea miembro de este convenio tiene que tener una legislación homogénea entre todos los países miembros y está estipulado en este convenio.

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa.

Premisa: Las entidades financieras se han adecuado a un proceso de globalización que conlleva a generar enormes cambios para la sociedad en consecuencia de los diversos delitos de la tecnología que infringen a la estabilidad y protección a nivel internacional; tanto de las personas jurídicas como naturales, presentándose bajo diferentes modalidades de sistemas o redes informáticas, generando una complejidad operativa y cambios constantes que dificultan su persecución.

04.- Según su punto de vista, ¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa?

La ley sanciona la comisión de los delitos informáticos y el hurto de dinero con el uso de la modalidad de phisging, las entidades financieras son las que no asumen responsabilidades y solo responsabilizan al cliente, esta respuesta tiene mucho que ver con lo que respuesta en la primera pregunta.

05.- La víctima de phishing es el sujeto pasivo, ignorante en tecnología y por ello es más vulnerable en los delitos cibernéticos; los cuales, se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica.

Dentro de su perspectiva, ¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?

No es necesario categorizar a la víctima ya que la modalidad de phisging, es una sola, y en los delitos informáticos se comete el delito desde que el ciberdelincuente envió el virus.

06.- Según sus erudiciones legales, ¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MPFN?

En la Ley 30086 y su modificatoria, se deben hacer cambios en la legislación y ser más específicos como estipular que el delincuente con el uso de información reservada de tarjetas o cuentas bancarias y la vulneración de claves secretas realiza transferencias ilícitas de dinero vía internet comete delito informático. Des eta forma la persona que son víctimas de phisging, estarían más protegidas.

Objetivo específico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras.

Premisa: Todo operador de justicia debe aprender el manejo de equipos actualizados ante la modernización de la delincuencia. El Ministerio Público tiene como meta orientar técnica y legalmente en las investigaciones de delitos informáticos, coordinando en todo el país con organismos estatales y privados.

07.- Explique ¿De qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?

Que el Ministerio Publico al tener una fiscalía especializada se capacite y trabaje en forma conjunta con la PNP y más que todo aprovechar la fragancia en esta modalidad.

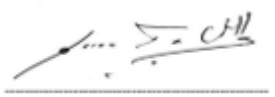
08.- ¿Qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?

Me parece una decisión del Ministerio Publico muy oportuna ya que las transferencias ilícitas de dinero vía internet por la modalidad de phishing, u otras modalidades de dinero son muy técnicas y requieren de personal de fiscales especializados o de lo contrario estos crímenes quedarían impunes.

09.- Una medida propuesta es la difusión de información por parte de las autoridades estatales y privadas a fin de propiciar la prevención del delito informático de Phishing, ¿Considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?

Si claro es la educación y la prevención que se debe internalizar en los clientes bancarios para evitar ser víctimas de fraudes informáticos por medio del phisging.

Firma:



JUAN ANTONIO POZO CASTILLO
DNI. 06222477

Entrevistado: Juan Antonio Pozo Castillo

DNI: 06222477

ANEXO 04: INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

Título: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Entrevistado/a:
Cargo/profesión/grado académico:
Normas básicas de la entrevista:

I. **INSTRUCCIONES:**

Leer detenidamente cada interrogante de la presente entrevista y responde desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: La protección a las víctimas de phishing hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, categorizados mayormente de forma errónea con la figura de "estafas"; por ello, que las entidades financieras buscan protegerse y también al usuario o consumidor a través de las normas establecidas; por tanto.

01.- Desde su experiencia profesional, diga Ud., ¿De qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?

La insuficiente tipificación del delito en el ámbito informático y su insuficiente control a nivel de legislación genera desprotección de las víctimas de Phishing.

02- El fraude informático es la vulneración del conjunto de reglas normativas sobre informática referente a todas sus manifestaciones. El artículo N°8 de la Ley N°30096 – Ley de Delitos Informáticos, señala en su primer párrafo al sujeto activo indicando las acciones ilícitas que serán reprimidas con una pena privativa de libertad o días multa; según su criterio, ¿Considera que la regulación vigente es eficiente para contrarrestar en los delitos de phishing?

Si, ya que contra los conductos que emplean o se hacen en sistemas informáticos se encuentran debidamente e individualmente tipificados en el ordenamiento jurídico.

03.- De acuerdo al Convenio de Budapest, el fraude informático está denominado como actos deliberados e ilegítimos que ocasionan perjuicio patrimonial a otro individuo, ¿Considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?

No, contra es necesario una regulación que sea específica y que recoja la sistematización de la realidad del avance de acuerdo al desarrollo informático alcanzado en el País.

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, Lima 2020.

Premisa: Las entidades financieras se han adecuado a un proceso de globalización que conlleva a generar enormes cambios para la sociedad en consecuencia de los diversos delitos de la tecnología que infringen a la estabilidad y protección a nivel

internacional; tanto de las personas jurídicas como naturales, presentándose bajo diferentes modalidades de sistemas o redes informáticas, generando una complejidad operativa y cambios constantes que dificultan su persecución.

04.- Según su punto de vista, ¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, Lima 2020?

Debido a la deficiencia normativa se utiliza este método del Phishing para engañar al agraviado y hacerle compartir contraseñas, números de tarjeta de crédito y otra información confidencial haciéndose pasar por una institución de confianza.

05.- La víctima de phishing es el sujeto pasivo, ignorante en tecnología y por ello es más vulnerable en los delitos cibernéticos; los cuales, se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica.

Dentro de su perspectiva, ¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?

Claro que sí es importantísimo categorizarlo para desagregar los contextos y poder discernir de nuevos tipos penales que pueden ser incluso distintos y más graves, a los cuales no los podrían vincular con una mayor punibilidad.

06.- Según sus erudiciones legales, ¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MPFN?

Se considera necesario el previo estudio de la realidad nacional para dar paso a la creación de diversos tipos penales

Objetivo especifico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: Todo operador de justicia debe aprender el manejo de equipos actualizados ante la modernización de la delincuencia. El Ministerio Público tiene como meta orientar técnica y legalmente en las investigaciones de delitos informáticos, coordinando en todo el país con organismos estatales y privados.

07.- Explique ¿De qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?

El Ministerio Público tiene el deber constitucional de poder perseguir el delito en este tipo de delitos. Sin embargo además puede actuar preventivamente mediante una Dirección de Prevención del delito.

08.- ¿Qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?

Me parece que el ciberdelito merece criterio especializado en materia penal y una capacitación bastante profunda en los delitos informáticos a nivel de fiscales y jueces.

09.- Una medida propuesta es la difusión de información por parte de las autoridades estatales y privadas a fin de propiciar la prevención del delito informático de Phishing. ¿Considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?

Es bueno del mayor control que tengan las empresas financieras en la prevención de este tipo de fraude y la actualización debido a el uso de las tecnologías de la información aparte de que incluya a el uso de tarjetas y claves

LUIS ALBERTO ALVAREZ TORRES

Entrevistado:

DNI: 41545422

D sfANEXO 04: INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

Titulo: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Entrevistado/a:Salvattore Leonardo Tripi Rossel
Cargo/profesión/grado académico: Magister en Derecho Procesal Penal
Normas básicas de la entrevista:

I. INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responde desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: La protección a las víctimas de phishing hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, categorizados mayormente de forma errónea con la figura de "estafas"; por ello, que las entidades financieras buscan protegerse y también al usuario o consumidor a través de las normas establecidas; por tanto.

01.- Desde su experiencia profesional, diga Ud., ¿De qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?

No es la ineficacia de las normas las que generan un problema en la protección de los usuarios y/o clientes de las entidades bancarias, son los niveles de seguridad de los procesos en las entidades bancarias que tienen problemas para la protección en contra de los casos de cibercrimen.

02- El fraude informático es la vulneración del conjunto de reglas normativas sobre informática referente a todas sus manifestaciones. El artículo N°8 de la Ley N°30096 – Ley de Delitos Informáticos, señala en su primer párrafo al sujeto activo indicando las acciones ilícitas que serán reprimidas con una pena privativa de libertad o días multa; según su criterio, ¿Considera que la regulación vigente es eficiente para contrarrestar en los delitos de phishing?

No existe el delito de phishing, es una modalidad de fraude cibernético. En materia penal la represión no implica un efecto de prevención, la razón de que la normativa establezca penas ínfimas se denota una ineficiente política criminal relacionada al cibercrimen, considerando además que el Estado Peruano es por lo pronto, ineficaz para la atención de los casos, toda vez que solo existe una división especializada de la policía DIVINDAT y no tiene homólogos en el Ministerio Público (que conozcan de la especialidad), hecho que genera un problema mucho mayor.

03.- De acuerdo al Convenio de Budapest, el fraude informático está denominado como actos deliberados e ilegítimos que ocasionan perjuicio patrimonial a otro individuo, ¿Considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?

El Estado Peruano para poder suscribir el convenio de Budapest, tuvo que incorporar y adecuar en su legislación lo relacionado al cibercrimen.

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, Lima 2020.

Premisa: Las entidades financieras se han adecuado a un proceso de globalización que conlleva a generar enormes cambios para la sociedad en consecuencia de los diversos delitos de la tecnología que infringen a la estabilidad y protección a nivel internacional; tanto de las personas jurídicas como naturales, presentándose bajo diferentes modalidades de sistemas o redes informáticas, generando una complejidad operativa y cambios constantes que dificultan su persecución.

04.- Según su punto de vista, ¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, Lima 2020?

La normativa no es ineficaz, el problema está en los operadores juridicos, me ratifico en el hecho que la problemática principal es la falta de seguridad que brindan las entidades financieras a a sus usuarios y/clientes.

05.- La víctima de phishing es el sujeto pasivo, ignorante en tecnología y por ello es más vulnerable en los delitos cibernéticos; los cuales, se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica.

Dentro de su perspectiva, ¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?

La categorización sería a nivel estadístico u otro que no tiene importancia penal, la legislación te establece que existe la victima y agraviado. Los bancos nunca te brindarían la cantidad amenazas cibernéticas, puesto que evidenciaría la vulneración en sus sistemas de seguridad.

06.- Según sus erudiciones legales, ¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MPFN?.

La normativa penal es especifica, algunas establecidas en el Código Penal y otras en normas accesorias que permiten al estado realizar las acciones correspondientes para investigar, procesar y sancionar los actos delictivos, no se puede establecer en forma especifica un tratamiento especial a una victima o agraviado por una modalidad de fraude cibernetico cuando la norma procesal establece su condición, no obstante, las victimas deben ser avalados por la entidad financiera correspondiente a quien se le ha vulnerado su sistema de seguridad, por ello los clientes se soportan en el prestigio y otros de la entidad financiera.

Objetivo específico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: Todo operador de justicia debe aprender el manejo de equipos actualizados ante la modernización de la delincuencia. El Ministerio Público tiene como meta orientar técnica y legalmente en las investigaciones de delitos informáticos, coordinando en todo el país con organismos estatales y privados.

07.- Explique ¿De qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?

No se entiende la pregunta.

08.- ¿Qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?

La administración de justicia se encuentra en sede del Poder Judicial, respecto del Ministerio Público, su actuación en cooperación con la PNP es muy importante, siempre y cuando conozcan de la especialidad, como lo mencioné en preguntas anteriores, la PNP no tiene un homologo en el MP especializado, si bien han creado Fiscalías para asumir el tema, esto no significa que existan personas que conozcan de la misma para asumir la investigación o estrategia legal para la investigación, lo cual, genera y generará siempre un peligro en la adecuada operatividad jurídica de la entidades encargadas.

09.- Una medida propuesta es la difusión de información por parte de las autoridades estatales y privadas a fin de propiciar la prevención del delito informático de Phishing, ¿Considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?

Considero, que toda acciones para mitir los fraudes ciberneticos deben ser impulsado a nivel privado y estatal, actyualmente los banco se aprovechan de sus

limitaciones en seguridad y obligan al cliente a asumir seguros para coberturas de fraudes cibernéticos, esto es un abuso privado que te genera un problema público, pues dejan de lado los casos ciberneticos solo porque ya nos son rentables, toda vez que el consumidor final adquirió un seguro que cubrirá el fraude, los más perjudicados son aquellos que no pueden adquirir dicho seguro.

Entrevistado:	Director de la Oficina de Asuntos Internos de la Oficina General de Integridad Institucional Ministerio del Interior. Salvattore Leonardo Tripi Rossel
DNI:	41437690

ANEXO 04: INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

Titulo: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Entrevistado/a:
Cargo/profesión/grado académico:
Normas básicas de la entrevista:

I. INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responde desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: La protección a las víctimas de phishing hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, categorizados mayormente de forma errónea con la figura de "estafas"; por ello, que las entidades financieras buscan protegerse y también al usuario o consumidor a través de las normas establecidas; por tanto.

01.- Desde su experiencia profesional, diga Ud., ¿De qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?

La normativa no regula procedimientos para la protección a las víctimas de phishing.

02- El fraude informático es la vulneración del conjunto de reglas normativas sobre informática referente a todas sus manifestaciones. El artículo N°8 de la Ley N°30096 – Ley de Delitos Informáticos, señala en su primer párrafo al sujeto activo indicando las acciones ilícitas que serán reprimidas con una pena privativa de libertad o días multa; según su criterio, ¿Considera que la regulación vigente es eficiente para contrarrestar los delitos informáticos en la modalidad de phishing?

No es suficiente, pero es una de las armas legales con el que se cuenta a la fecha para hacer frente el fraude informático, y poder frenar el cibercrimen que se viene incrementando a través de sus diversas modalidades.

03.- De acuerdo al Convenio de Budapest, el fraude informático está denominado como actos deliberados e ilegítimos que ocasionan perjuicio patrimonial a otro individuo, ¿Considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?

Efectivamente, en la Ley de Delitos Informáticos, se recoge las consideraciones del Art. 8 del Convenio de Budapest.

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa.

Premisa: Las entidades financieras se han adecuado a un proceso de globalización que conlleva a generar enormes cambios para la sociedad en consecuencia de los diversos delitos de la tecnología que infringen a la estabilidad y protección a nivel internacional; tanto de las personas jurídicas como naturales, presentándose bajo diferentes modalidades de sistemas o redes informáticas, generando una complejidad operativa y cambios constantes que dificultan su persecución.

04.- Según su punto de vista, ¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa?

No existe una vulneración a las víctimas de phishing en entidades financieras que esté relacionado a la normativa.

05.- La víctima de phishing es el sujeto pasivo, ignorante en tecnología y por ello es más vulnerable en los delitos cibernéticos; los cuales, se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica.

Dentro de su perspectiva, ¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?

El phishing es una de las modalidades mas frentes al que recurre el ciberdelincuente para la obtención de información confidencial, que incrementan de una mancera acelerada los delitos informáticos.

06.- Según sus erudiciones legales, ¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MPFN?

Se debe entender que el phishing es una modalidad para la obtención de información confidencial, pero puede ser utilizado no solo con entidades sociales sino en diferentes escenarios que ofrece el ciberespacio, por lo tanto, consideró la formalización de la denuncia se da por el tipo penal y no por la modalidad (phishing).

Objetivo específico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras.

Premisa: Todo operador de justicia debe aprender el manejo de equipos actualizados ante la modernización de la delincuencia. El Ministerio Público tiene como meta orientar técnica y legalmente en las investigaciones de delitos informáticos, coordinando en todo el país con organismos estatales y privados.

07.- Explique ¿De qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?

Desconozco la actuación del Ministerio Público para la protección a las víctimas de phishing.

08.- ¿Qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?

De gran importancia porque va a permitir hacer frente de manera articulada el cibercrimen, incluyendo a víctimas de phishing.

09.- Una medida propuesta es la difusión de información por parte de las autoridades estatales y privadas a fin de propiciar la prevención del delito informático de Phishing, ¿Considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?

La prevención es importante para a dar a conocer a la ciudadanía que cada vez es más digital de los peligros al que esta expuesto y modalidades existentes al que recurre el ciberdelincuente para obtener información confidencial.

Firma:

Entrevistado: Wuilman Zabarburu Vargas

DNI: 40072448

ANEXO 04: INSTRUMENTO DE RECOLECCIÒN DE DATOS

GUIA DE ENTREVISTA

Titulo: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Entrevistado/a: Nino Alvarez Rios
Cargo/profesión/grado académico: Abogado
Normas básicas de la entrevista:

I. INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responde desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: La protección a las víctimas de phishing hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, categorizados mayormente de forma errónea con la figura de "estafas"; por ello, que las entidades financieras buscan protegerse y también al usuario o consumidor a través de las normas establecidas; por tanto.

01.- Desde su experiencia profesional, diga Ud., ¿De qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?

Los efectos que genera la ineficacia normativa contra la protección a las víctimas de phishing se evidencian en el día a día de esta coyuntura social que resaltó estos casos con los bonos del gobierno, aunado a ello el desconocimiento de la norma hace que las entidades estatales interpreten de manera errónea esta modalidad confundiéndola con estafas.

02- El fraude informático es la vulneración del conjunto de reglas normativas sobre informática referente a todas sus manifestaciones. El artículo N°8 de la Ley N°30096 – Ley de Delitos Informáticos, señala en su primer párrafo al sujeto activo indicando las acciones ilícitas que serán reprimidas con una pena privativa de libertad o días multa; según su criterio, ¿Considera que la regulación vigente es eficiente para contrarrestar los delitos informáticos en la modalidad de phishing?

Sobre la regulación vigente, es preciso indicar que ésta no es eficiente, toda vez que a pesar de señalar las acciones ilícitas que conllevan a una sanción penal, no establece todas las modalidades de los delitos cibernéticos e incluso resalta para muchos abogados una ambigüedad de la norma al no reconocer semejanzas entre delitos informáticos y cibernéticos, dejando de lado las modalidades que han ido apareciendo progresivamente en nuestro país.

03.- De acuerdo al Convenio de Budapest, el fraude informático está denominado como actos deliberados e ilegítimos que ocasionan perjuicio patrimonial a otro individuo, ¿Considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?

Actualmente, nuestro país se encuentra suscrito al Convenio de Budapest y si han sido consideradas en nuestro marco legal; sim embargo, la realidad es la falta de capacitación del personal judicial y policial que observan estos casos, así mismo, no se ha considerado al detalle las diferentes figuras de delitos cibernéticos y mucho menos se ha conceptualizado concretamente estos actos ilícitos.

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, Lima 2020.

Premisa: Las entidades financieras se han adecuado a un proceso de globalización que conlleva a generar enormes cambios para la sociedad en consecuencia de los diversos delitos de la tecnología que infringen a la estabilidad y protección a nivel internacional; tanto de las personas jurídicas como naturales, presentándose bajo

diferentes modalidades de sistemas o redes informáticas, generando una complejidad operativa y cambios constantes que dificultan su persecución.

04.- Según su punto de vista, ¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, Lima 2020?

La vulneración de protección a las víctimas de phishing se realiza cuando no se respeta el bien jurídico protegido de toda persona, en estos casos se hace mención al patrimonio, integridad, confidencialidad y disponibilidad de información de las víctimas, quienes se perjudican y pierden la confianza en el sistema judicial para la resolución de estos delitos; ya que, el presunto denunciado tiene acceso a sitios web que perjudicarían al denunciante y al no ser procesado por falta de pruebas, mala formulación de denuncias o pericias mal ejecutadas; todo ello conllevaría a la falta de protección y falta de políticas públicas en estos delitos.

05.- La víctima de phishing es el sujeto pasivo, ignorante en tecnología y por ello es más vulnerable en los delitos cibernéticos; los cuales, se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica.

Dentro de su perspectiva, ¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?

Sí, es necesario tener un amplio panorama de las cifras actuales de estos hechos delictivos que permitirían prevenir e identificar quienes son las personas más vulnerables a ser víctimas, así también se diferenciaría cada modalidad y esto conllevaría a conceptualizar mejor para realizar sanciones concretas y específicas; ya que la DIVINDAT, solo tiene datos generales realizados en base a las denuncias formuladas más no existe cifras de cada modalidad cibernética y en muchas casos son confundidas con la figura delictiva de estafas.

06.- Según sus erudiciones legales, ¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MPFN?

La Ley N°30096, debe ser modificada porque como bien mencioné anteriormente no precisa el concepto de estas modalidades y mucho menos aclara la diferencia entre delitos informáticos, cibernéticos y estafas; además, debe considerarse capacitar al personal judicial y policial, que muchas veces desconocen de estos temas y se encuentran laborando en el área de ciberdelitos.

Objetivo específico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: Todo operador de justicia debe aprender el manejo de equipos actualizados ante la modernización de la delincuencia. El Ministerio Público tiene como meta orientar técnica y legalmente en las investigaciones de delitos informáticos, coordinando en todo el país con organismos estatales y privados.

07.- Explique ¿De qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?

El Ministerio Público, ha buscado contrarrestar estos delitos creando una nueva fiscalía, la cual es la única a nivel nacional que en la realidad no se abastece y además desconoce de la realidad problemática, así como el personal no está calificado por falta de especializaciones, conocimientos informáticos y legales.

08.- ¿Qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?

Me parece una gran iniciativa, siempre que el gobierno aporte con políticas públicas y presupuesto para llevar a cabo regularmente las capacitaciones del personal, porque si dejamos de lado esto sería como tener un caballo blanco, inservible para la población.

09.- Una medida propuesta es la difusión de información por parte de las autoridades estatales y privadas a fin de propiciar la prevención del delito informático de Phishing, ¿Considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?

Considero que si podría ayudar la educación a la población sobre estos hechos; sin embargo, la interpretación de la norma se rige en base a nuestros administradores de justicia y son ellos quienes también deben recibir la información correspondiente en base a la Ley N°30096. Además, centrándose en la modalidad de phishing debe considerarse que las entidades financieras también forman parte de estos hechos, en algunas ocasiones son víctimas y otras veces son utilizadas como medio de suplantación por otros sitios web, es así que debe considerarse una política al usuario de prevención ante estos hechos.

Firma:

Entrevistado: Nino Alvarez Rios

DNI:42365302

ANEXO 04: INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

Titulo: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Entrevistado/a: Gustavo Vilchez Cordero
Cargo/profesión/grado académico: Abogado
Normas básicas de la entrevista:

I. INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responde desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: La protección a las víctimas de phishing hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, categorizados mayormente de forma errónea con la figura de "estafas"; por ello, que las entidades financieras buscan protegerse y también al usuario o consumidor a través de las normas establecidas; por tanto.

01.- Desde su experiencia profesional, diga Ud., ¿De qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?

…Que, debería ver más conocimientos en informática por parte de las personas porque muy fácilmente hacer transacciones tecnológicas sin tener el total conocimiento de la informática, por ello es importante que las autoridades estén más atentos a estos señores denominados HACKER. Y por ello con la intervención policial deberá desarticular esta organización criminal que tanto daño hace a los usuarios del sistema bancario.

02- El fraude informático es la vulneración del conjunto de reglas normativas sobre informática referente a todas sus manifestaciones. El artículo N°8 de la Ley N°30096 – Ley de Delitos Informáticos, señala en su primer párrafo al sujeto activo indicando las acciones ilícitas que serán reprimidas con una pena privativa de libertad o días multa; según su criterio, ¿Considera que la regulación vigente es eficiente para contrarrestar en los delitos de phishing?

…Que, en relación a este punto si bien he cierto es importante las penas, para mi concepto el aumento de las penas no es la solución al problema, lo que debería realizarse es un estudio minucioso y poder encontrar una solución a los problemas informaticos,es por ello que el gobierno central debería de dar mayores alcances y conocimientos tecnológicos para el mayor conocimiento de los mecanismos de tecnología y así poder ayudar a la sociedad de esta lacra social que tanto daño hace a nuestros usuarios.

03.- De acuerdo al Convenio de Budapest, el fraude informático está denominado como actos deliberados e ilegítimos que ocasionan perjuicio patrimonial a otro individuo, ¿Considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?

A mi concepto como abogado litigante, no lo han tenido en cuenta al momento de calificar el presente convenio, porque está vulnerando varios derechos como por ejemplo el de ayudar a las personas a poder manejar el sistema informático de una manera no muy usual, y el estado debería de ayudar a las personas a poder manejar este programa ya que muchas personas son víctimas de fraudes informáticos entre otros.

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, Lima 2020.

Premisa: Las entidades financieras se han adecuado a un proceso de globalización que conlleva a generar enormes cambios para la sociedad en consecuencia de los diversos delitos de la tecnología que infringen a la estabilidad y protección a nivel internacional; tanto de las personas jurídicas como naturales, presentándose bajo diferentes modalidades de sistemas o redes informáticas, generando una complejidad operativa y cambios constantes que dificultan su persecución.

04.- Según su punto de vista, ¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, Lima 2020?

Que, lo sucedido a muchas personas que desconocen el movimiento de informática de buena fe, le envían mensajes y este al mismo tiempo le envían y dan un clik, con esto están siendo jakeados, con sus cuentas corrientes y están está siendo vaciados todo su dinero, por ello es importante que el banco le dé seguridad al momento de abrir una cuenta corriente, por ello ahora se está implementando un programa de seguro de su tarjeta, pero que se tendrá que realizar su trámite en el Banco.

05.- La víctima de phishing es el sujeto pasivo, ignorante en tecnología y por ello es más vulnerable en los delitos cibernéticos; los cuales, se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica.

Dentro de su perspectiva, ¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?

Que, si es importante establecer los sujetos tanto pasivo, como activo, por ello es importante que las normas como lo he manifestado sean más drásticas y no tengan ningún beneficio, para que estas personas que hacen daño no cometan delito y no puedan dañar a los usuarios.

06.- Según sus erudiciones legales, ¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MPFN?.

Que, si bien existe una norma esta debería ser mas drástica, porque esta pena es muy blanca y con ello aplicando la Terminación Anticipada o la Conclusión Anticipada esta le reducirá la pena y ahí mismo se le pondrá en libertad, sin embargo si las penas son más gravosas y así se acoja a estos procesos especiales no llegara a una pena menor de 4 años y será efectiva, por ello solicito que las penas sean más duras.

Objetivo específico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: Todo operador de justicia debe aprender el manejo de equipos actualizados ante la modernización de la delincuencia. El Ministerio Público tiene como meta orientar técnica y legalmente en las investigaciones de delitos informáticos, coordinando en todo el país con organismos estatales y privados.

07.- Explique ¿De qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?

Que, el ministerio público, como titular de la acción penal publica, deberá de investigar la investigación y si durante la investigación ha encontrado alguna responsabilidad tendrá que formalizar denuncia penal y posteriormente estaríamos inmerso en un proceso penal por el presunto delito de delitos informáticos y otros.

08.- ¿Qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?

…Que, me parece importante de que el gobierno se preocupe por estos delitos, si bien he cierto se ha creado fiscalías especializadas, es muy bien cierto que estos despachos realizaran sus labores de investigación y formulación de denuncias al haber encontrado en algún etapa de investigar si amerita una denuncia penal, como representante del Ministerio Publico. Como titubar de la acción penal pública.

09.- Una medida propuesta es la difusión de información por parte de las autoridades estatales y privadas a fin de propiciar la prevención del delito informático de Phishing, ¿Considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?

…Que, el gobierno deberia de dar mas informacion a las personas con relacion a los delincuentes que ingresan a sus cuentas con el propósito de ingresar a su cuenta y dejarlos sin ningun ahorro por parte de los usuarios, es por ello, que el gobierno central intervenga en este flagelo que tanto daño hace al pais y a las personas.

Entrevistado: Gustavo Vilchez Cordero. Abogado C.A.L. Reg. Nº 46450.

DNI:09443206

ANEXO 04: INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

Titulo: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Entrevistado/a:JUAN JOSE PAREDES CORDERO
Cargo/profesión/grado académico:ABOGADO
Normas básicas de la entrevista:

I. **INSTRUCCIONES:**

Leer detenidamente cada interrogante de la presente entrevista y responde desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: La protección a las víctimas de phishing hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, categorizados mayormente de forma errónea con la figura de "estafas"; por ello, que las entidades financieras buscan protegerse y también al usuario o consumidor a través de las normas establecidas; por tanto.

01.- Desde su experiencia profesional, diga Ud., ¿De qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?

En realidad, no es por falta de normativa, sino lo que pasa es que esta modalidad delictiva afecta directamente a los bancos y sus clientes, siendo así que ellos mismos se encargan de su investigación, actualmente apoyados por la policía especializada, pero a medida que avanza la tecnología siguen apareciendo modalidades conexas, pero si cabe que se actualicen las normativas legales al respecto.

02- El fraude informático es la vulneración del conjunto de reglas normativas sobre informática referente a todas sus manifestaciones. El artículo N°8 de la Ley N°30096 – Ley de Delitos Informáticos, señala en su primer párrafo al sujeto activo indicando las acciones ilícitas que serán reprimidas con una pena privativa de libertad o días multa; según su criterio, ¿Considera que la regulación vigente es eficiente para contrarrestar en los delitos de phishing?

La vigente no, por cuanto siguen apareciendo delitos conexos directamente vinculado al phishing, tanto es así que diferentes entidades han tomado nota y han elaborado planes o directivas para contrarrestar este tipo de delito.

03.- De acuerdo al Convenio de Budapest, el fraude informático está denominado como actos deliberados e ilegítimos que ocasionan perjuicio patrimonial a otro individuo, ¿Considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?

Si, pero como lo vengo repitiendo al existir delitos conexos directamente vinculados al delito principal o más antiguo, la normativa debe actualizarse e ir a la par a medida que avanza la tecnología cibernética.

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, Lima 2020.

Premisa: Las entidades financieras se han adecuado a un proceso de globalización que conlleva a generar enormes cambios para la sociedad en consecuencia de los diversos delitos de la tecnología que infringen a la estabilidad y protección a nivel internacional; tanto de las personas jurídicas como naturales, presentándose bajo diferentes modalidades de sistemas o redes informáticas, generando una complejidad operativa y cambios constantes que dificultan su persecución.

04.- Según su punto de vista, ¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, Lima 2020

Efectivamente, la normativa no favorece o establece medidas de protección al cliente, salvo la responsabilidad civil de las entidades bancarias, pero cuya investigación la hacen ellos. ósea las Entidades Financieras son juez y parte en este tipo de delitos, que definitivamente va a favorecerlo a ellos.

05.- La víctima de phishing es el sujeto pasivo, ignorante en tecnología y por ello es más vulnerable en los delitos cibernéticos; los cuales, se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica.

Dentro de su perspectiva, ¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?

Lo que realmente debe hacerse es realizar campañas de información a los clientes, para que conozcan este tipo de delitos, pero sobre todo tiene que hacerse programas o planes en las mismas entidades financieras y crear medidas de seguridad informática en favor de sus clientes.

06.- Según sus erudiciones legales, ¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MP?.

Definitivamente que si, es necesario que las investigaciones por este este tipo delitos incluido la responsabilidad o no de la entidad financiera y responsabilidad civil, la realice la policía especializada, para que esta se realice en forma imparcial en beneficio de los clientes , porque estos al final resultan víctimas, porque muchas veces la entidad financiera quiere hacer responsable al cliente.

Objetivo específico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: Todo operador de justicia debe aprender el manejo de equipos actualizados ante la modernización de la delincuencia. El Ministerio Público tiene como meta orientar técnica y legalmente en las investigaciones de delitos informáticos, coordinando en todo el país con organismos estatales y privados.

07.- Explique ¿De qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?

EL MP como defensor del ciudadano, debe orientar y como Entidad mediante sus facultades para la promulgación de leyes, normas actualizadas al respecto, porque si no, no tiene las herramientas jurídicas actualizadas poco o nada puede hacer en la lucha contra este tipo de delito.

08.- ¿Qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?

Es una medida adecuada por la especialización, pero esta debe ir de la mano de la policía especializada y de las normas jurídicas que avalen su trabajo, sobre todo que tiene que actualizarse constantemente y conocer sobre estos tipos de delitos.

Una medida propuesta es la difusión de información por parte de las autoridades estatales y privadas a fin de propiciar la prevención del delito informático de Phishing, ¿Considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?

Si bien seria una buena medida, pero los delitos van dirigidos a las pocas medidas de seguridad que tienen las entidades financieras para resguardar la identidad y las cuentas de sus clientes.

Entrevistado: ABOGADO JUAN JOSE PAREDES CORDERO

DNI: 06006725 CAL 48796

ANEXO 04: INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

Titulo: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Entrevistado/a: Jorge Fernando Del Rio Espinoza
Cargo/profesión/grado académico: Abogado.
Normas básicas de la entrevista:

I. **INSTRUCCIONES:**

Leer detenidamente cada interrogante de la presente entrevista y responde desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: La protección a las víctimas de phishing hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, categorizados mayormente de forma errónea con la figura de "estafas"; por ello, que las entidades financieras buscan protegerse y también al usuario o consumidor a través de las normas establecidas; por tanto.

01.- Desde su experiencia profesional, diga Ud., ¿De qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?

IMPIDE UNA EFICAZ Y ADECUADA REPRESIÓN DE ESTAS CONDUCTAS LO CUAL ORIGINA DESPROTECCIÓN DE LA ACTIVIDAD ECONÓMICA Y EMPRESARIAL. VIENDOSE MENOSCABADO EL JUSTO DERECHO DE LAS VÍCTIMAS A LA ADECUADA PRESERVACIÓN DE SUS DATOS DE IDENTIDAD.

02- El fraude informático es la vulneración del conjunto de reglas normativas sobre informática referente a todas sus manifestaciones. El artículo N°8 de la Ley N°30096 – Ley de Delitos Informáticos, señala en su primer párrafo al sujeto activo indicando las acciones ilícitas que serán reprimidas con una pena privativa de libertad o días multa; según su criterio, ¿Considera que la regulación vigente es eficiente para contrarrestar los delitos informáticos en la modalidad de phishing?

NO, PORQUE PRESCINDE PRECISAMENTE DEL FACTOR ENGAÑO y/o INDUCIR A ERROR PARA EL ACCESO PRIVILEGIADO A INFORMACIÓN DE CARÁCTER RESERVADA. ESCENARIO SUBSUMIDO EN LA MODALIDAD DEL PHISHING.

03.- De acuerdo al Convenio de Budapest, el fraude informático está denominado como actos deliberados e ilegítimos que ocasionan perjuicio patrimonial a otro individuo, ¿Considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?

ESTÁN RECOGIDOS OTRINCIPALMENTE PUES SE ENFOCA EL COMPONENTE DOLITIVO Y ANTIJURÍDICO DE LA CONDUCTA, EMPERO NO SE HA PROCURADO ADECUAR LA NORMA DE SU PROPÓSITO A ESTOS NUEVOS TIPOS DELICTIVOS.

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa.

Premisa: Las entidades financieras se han adecuado a un proceso de globalización que conlleva a generar enormes cambios para la sociedad en consecuencia de los diversos delitos de la tecnología que infringen a la estabilidad y protección a nivel internacional; tanto de las personas jurídicas como naturales, presentándose bajo

diferentes modalidades de sistemas o redes informáticas, generando una complejidad operativa y cambios constantes que dificultan su persecución.

04.- Según su punto de vista, ¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa?

LA MODALIDAD, FRAUDULENTO DEL PHISHING SE ORIENTO A SUPLANTAR LO IDENTIDAD DEL USUARIO PARA APROPIARSE DE SUS DATOS CONFIDENCIALES, ESTO PONE EN PELIGRO LA INTEGRIDAD DE DICHA INFORMACIÓN SENSIBLE POR SU NATURALEZA, Y QUE DADO EL CONTEXTO DE SU MANIFESTACIÓN, PODRÍA TORNARSE INJUSTO IMPUNE. POR CUESTIONES RELATIVAS A MODERNIZACIÓN DE LA LEGISLACIÓN.

05.- La víctima de phishing es el sujeto pasivo, ignorante en tecnología y por ello es más vulnerable en los delitos cibernéticos; los cuales, se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica.

Dentro de su perspectiva, ¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?

POR SUPUESTO, ES FUNDAMENTAL, PUES A PARTIR DE ELLO, SE OBTENDRÁ INFORMACIÓN FIDEDIGNA QUE COADYUBE A IDENTIFICAR LA PELIGROSIDAD DE ESTAS CONDUCTAS, Y EL COMPORTAMIENTO DEL USUARIO FRENTE A DICHO ESCENARIO.

06.- Según sus erudiciones legales, ¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MPFN?

CLARO, EN UN MARCO INTEGRADO DE ATENCIÓN AL PRINCIPIO DE LEGALIDAD, SE DEBE PROCURAR QUE CONDUCTAS COMO LAS ENUNCIADAS SE ENCUENTREN PREESTABLECIDAS EN UN DISPOSITIVO CON RANGO DE LEY MÁS AÚN, SI EN LA ACTUALIDAD REPRESENTA UNA DE LAS TÉCNICAS MÁS EMPLEADAS PARA HURTAR INFORMACIÓN A TRAVÉS DE INTERNET.

Objetivo específico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras.

Premisa: Todo operador de justicia debe aprender el manejo de equipos actualizados ante la modernización de la delincuencia. El Ministerio Público tiene como meta orientar técnica y legalmente en las investigaciones de delitos informáticos, coordinando en todo el país con organismos estatales y privados.

07.- Explique ¿De qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?

CON EL DESARROLLO DE NUEVAS TECNOLOGÍAS, HA SURGIDO UN INCREMENTO DE LA CIBERDELINCUENCIA, PARA ESTE EFECTO EL MINISTERIO HA CREADO LA UNIDAD FISCAL ESPECIALIZADA EN DICHA MATERIA, PROCURANDO DESDE UNA ORIENTACIÓN TÉCNICO JURÍDICA EN LA INVESTIGACIÓN: LA PRESERVACIÓN DE LA EVIDENCIA DIGITAL, APLICANDO Y PROPONIENDO DIRECTIVAS, LINEAMIENTOS, INSTRUCTIVOS Y GUÍAS EN EL MARCO DE SU COMPETENCIA.

08.- ¿Qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?

ADECUADO PARA LA PROBLEMÁTICA EXISTENTE, CONSIDERANDO QUE DESDE EL 27 DE OCTUBRE DE 2013 AL 31 DE JULIO DE 2020 FUERON 6 FISCALÍAS UN TOTAL 21,687 DENUNCIAS POR DELITOS INFORMÁTICOS, POCO CONOCIMIENTO CORRESPONDERÍA A ESTA UNIDAD ESPECIALIZADA QUE POR SU CAPACIDAD DOTARÁ DE MAYOR EFICACIA EL RECOJO DE INDICIOS Y PRESERVACIÓN DE LA EVIDENCIA.

09.- Una medida propuesta es la difusión de información por parte de las autoridades estatales y privadas a fin de propiciar la prevención del delito

informático de Phishing, ¿Considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?

POR SUPUESTO, UNA ADECUADA EDUCACIÓN TECNOLÓGICA GARANTIZA EL CARÁCTER PREVENTIVO DE LA NORMA, Y COMO CONSECUENCIA DE ELLO, TORNARÍA MÁS EFECTIVA SU EFICIENCIA, COBERTURANDO EN UN ÁMBITO TÉCNICO LA TIPICIDAD DE LA CONDUCTA.

Firma:

Entrevistado: JORGE FERNANDO DEL RÍO ESPINOZA.

DNI: 43111973

ANEXO 04: INSTRUMENTO DE RECOLECCIÓN DE DATOS

GUIA DE ENTREVISTA

Titulo: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Entrevistado/a: Victor Eduardo Augusto Moran Leon
Cargo/profesión/grado académico:
Normas básicas de la entrevista:

I. INSTRUCCIONES:

Leer detenidamente cada interrogante de la presente entrevista y responde desde su experiencia, conocimiento opinión, con claridad y veracidad sus respuestas, debido que, las respuestas consignadas, serán el fundamento para validar nuestra hipótesis de trabajo y corroborar nuestros objetivos.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Premisa: La protección a las víctimas de phishing hace referencia a la población afectada por este ciberdelito que se direcciona a sistemas o redes informáticas, categorizados mayormente de forma errónea con la figura de "estafas"; por ello, que las entidades financieras buscan protegerse y también al usuario o consumidor a través de las normas establecidas; por tanto.

01.- Desde su experiencia profesional, diga Ud., ¿De qué manera la ineficacia normativa genera efectos contra la protección a las víctimas de phishing en entidades financieras, Lima 2020?

En la actualidad uno de los objetivos de la norma (prevenir) no ha sido cumplido, pues no se han efectuado los mecanismos idóneos para la protección de datos de las personas en entidades financieras. Así mismo, como el fraude informático propiamente dicho previsto en código penal y en la Ley 30096 es abarcado de manera amplia, generando vacíos legales que permiten que las entidades no se hagan responsables por el aseguramiento de los datos de clientes.

02- El fraude informático es la vulneración del conjunto de reglas normativas sobre informática referente a todas sus manifestaciones. El artículo N°8 de la Ley N°30096 – Ley de Delitos Informáticos, señala en su primer párrafo al sujeto activo indicando las acciones ilícitas que serán reprimidas con una pena privativa de libertad o días multa; según su criterio, ¿Considera que la regulación vigente es eficiente para contrarrestar los delitos informáticos en la modalidad de phishing?

No, toda vez que este tipo de acto ilícito ha ido evolucionando en el tiempo, sin que se haya previsto normativamente un modelo de protección para las personas.

03.- De acuerdo al Convenio de Budapest, el fraude informático está denominado como actos deliberados e ilegítimos que ocasionan perjuicio patrimonial a otro individuo, ¿Considera usted que las sanciones impuestas en el Convenio de Budapest para los nuevos tipos delictivos sobre la utilización de las tecnologías informáticas en entidades financieras han sido recogidas en la regulación actual?

No, pues aún no se encuentra legislada las sanciones en contra de las personas jurídicas que se encontraran responsables.

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa.

Premisa: Las entidades financieras se han adecuado a un proceso de globalización que conlleva a generar enormes cambios para la sociedad en consecuencia de los diversos delitos de la tecnología que infringen a la estabilidad y protección a nivel internacional; tanto de las personas jurídicas como naturales, presentándose bajo diferentes modalidades de sistemas o redes informáticas, generando una complejidad operativa y cambios constantes que dificultan su persecución.

04.- Según su punto de vista, ¿Cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa?

A la fecha las entidades financieras no han generado una protección adecuada de los datos de los clientes, por cuanto no existe una sanción para ellos, la norma si bien tiene como objeto prevenir el delito, esto no se ha cumplido, debido también a las innovaciones tecnológicas que se implementan para los hechos delictivos.

05.- La víctima de phishing es el sujeto pasivo, ignorante en tecnología y por ello es más vulnerable en los delitos cibernéticos; los cuales, se ejecutan a través de medios informáticos que no acatan lo estipulado en la norma, buscando perjudicar los dispositivos informáticos, redes o cualquier otra herramienta de comunicación electrónica.

Dentro de su perspectiva, ¿Es necesario categorizar a las víctimas de phishing para identificar y contrarrestar las modalidades más frecuentes obteniendo datos reales del incremento acelerado en delitos informáticos?

Si.

06.- Según sus erudiciones legales, ¿Considera que en la Ley N°30096, debería implementarse nuevas normativas a favor de las víctimas de phishing en entidades financieras para una mejor formalización de denuncia por parte del MPFN?

No.

Objetivo específico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras.

Premisa: Todo operador de justicia debe aprender el manejo de equipos actualizados ante la modernización de la delincuencia. El Ministerio Público tiene como meta orientar técnica y legalmente en las investigaciones de delitos informáticos, coordinando en todo el país con organismos estatales y privados.

07.- Explique ¿De qué manera puede identificar la actuación del Ministerio Público para la protección a las víctimas de phishing en entidades financieras, contra la ineficacia normativa?

El ministerio público como seguidor del delito, no establece protección a la víctima pues la denuncia e investigación se efectúa después de cometido el delito.

08.- ¿Qué opinión le merece, la implementación de despachos fiscales penales con autoridades especializadas en delitos cibernéticos para la debida administración de justicia que conozcan y resuelvan este tipo de delito que involucra a víctimas de phishing en entidades financieras?

La especialización de despachos fiscales en delitos cibernéticos hace que se implementen la normativa específica para cada caso y en consecuencia las sanciones sean las adecuadas, así mismo, promueve una estadística de los casos con los que se podrán materializar nuevas normativas que permitan contrarrestar este delito.

09.- Una medida propuesta es la difusión de información por parte de las autoridades estatales y privadas a fin de propiciar la prevención del delito informático de Phishing, ¿Considera usted, que tal medida garantizará la eficacia y eficiencia de la interpretación de la norma?

Si, cuanto más conocimiento tome la población de nuevas modalidades de estafas cibernéticas, estarán más atentos en no caer en ellas.

Firma:

Victor Eduardo Augusto Moran Leon – ICAP 3047
Asesor 2 del congresista César Manuel Revilla Villanueva

Entrevistado:

UNIVERSIDAD CÉSAR VALLEJO

ANEXO 08

INSTRUMENTO DE RECOLECCIÓN DE DATOS

FICHA DE ANÁLISIS DE FUENTE DOCUMENTAL

Título: Ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

Objetivo general

Analizar los efectos que genera la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

I. ANÁLISIS DE JURISPRUDENCIA INTERNACIONAL

FUENTE DOCUMENTAL	Consejo General del Poder Judicial de Logroño de España. https://www.poderjudicial.es/search/doAction?action=contentpdf&databasematch=AN&reference=7095915&links="phishing"&optimize=20140613&publicinterface=true
CONTENIDO DE LA FUENTE A ANALIZAR	La apelación de procedimiento abreviado resuelve en la sentencia N°77/2014 que fue emitido en fecha 16 de abril del 2014 por el Consejo General del Poder Judicial de Logroño de España, el cual versa sobre la sentencia del Juzgado Penal Nº2 de Logroño cuya decisión fue condenar a los autores responsables del delito de estafa penal, en su modalidad de phishing, por haber efectuado una manipulación informática con el fin de conseguir la transferencia no consentida por lo que se estaría realizando la acción ilícita propuesta en artículo 248.2 numeral a), debiendo indemnizar al BANCO BILBAO VIZCAYA ARGENTARIA, S.A. más los intereses señalados en el artículo 576 de la Ley de Enjuiciamiento Civil. Sim embargo, en la apelación los autores alegaron su inocencia, negando ser autor o cooperador de la estafa informática y la vulneración del principio in dubio pro reo e indebida aplicación del artículo 248.2 a) del Código Penal; por ello, la Sala en su fallo desestima el recurso de apelación de Hermenegildo y estima parcialmente el recurso de apelación de Lorenzo.
ANÁLISIS DEL CONTENIDO	Vale decir, los autores responsables de este ilícito plantearon su apelación de la sentencia tratando de desvirtuar la autoría, alegando así una indebida aplicación del artículo antes referido, por lo que expresan no haber cometido el delito del articulo 248.2 a) del Código Penal y no ser autores de dicho delito de informático según lo que expresan. Es así, que el pronunciamiento de la apelación queda desestimada en parte para Lorenzo, al demostrarse que no es cooperador necesario de un delito consumado, ya que el delito quedó en grado de tentativa como lo indica el artículo 16 del Código Penal: “hay tentativa cuando el sujeto da principio a la ejecución del delito directamente por hechos exteriores, practicando todos o parte de los actos que objetivamente deberían de producir el resultado, y sin embargo éste no se produce por causas independientes de la voluntad del autor.” Demostrándose haber tenido la tentativa acabada frente a la recepción de transferencia de la cuenta BBVA, porque el acusado llegó a retirar el dinero de su cuenta y posterior a la llamada de su jefe inmediato decide reintegrar el dinero al banco.

	La Sala manifiesta no estar completamente de acuerdo con la sentencia y por ello en el fallo especifican que autor es ratificado en su condena y en el caso de Lorenzo expresan que en lugar de un año impuesto en la sentencia apelada tendrá cuatro meses de prisión.

PONDERAMIENTO DE LAS INVESTIGADORAS / CONCLUSIÓN

En la presente jurisprudencia internacional, respecto al **punto tercero y el fallo impuesto en el procedimiento penal – apelación del procedimiento abreviado por el Consejo General del Poder Judicial de Logroño de España (SAP LO 233/2014)** que versa sobre la sentencia del Juzgado Penal de Logroño; nos enfocaremos en el señor Lorenzo quien ha tratado de desvirtuar su accionar indicando que hubo una mala aplicación del artículo 248.2 a) del Código Penal, manifestando que no efectuó ninguna manipulación informática ni ha conseguido una transferencia no consentida, así mismo dijo que se vulneró su derecho a la presunción de inocencia, de esto señalamos que resulta impropio y carece de veracidad dado que se demostró que el autor tiene conocimiento de la propia acción y las consecuencias que genera dicho acto.

Pero, conforme la jurisprudencia la Sala ha indicado en el tercer párrafo del punto tercero de la sentencia sobre apelación del procedimiento abreviado que no está de acuerdo con la calificación de cooperador necesario de un delito consumado; ya que el acusado no consumó el delito de acuerdo a los actos descritos y lo establecido en la norma de España. Por ende, las acciones ilícitas realizadas por el autor configuradas en la aplicación de las normas en los casos de modalidades de phishing, se puede concluir que en el presente caso del señor Lorenzo existió una ineficacia normativa; ya que, la norma impuesta para el acto ilícito efectuado por el acusado era específica y concreta, pero no fue eficaz; toda vez que el administrador de justicia que impuso la sentencia en el Juzgado Penal, no consideró el grado de tentativa y la pena impuesta en el artículo 62 del Código Penal; evidenciando la falta de conocimiento legal, interpretación de la norma, y los efectos legales de la ineficacia normativa, que en este caso correspondió a una pena de prisión como autor responsable de un delito de estafa informática en modalidad de phishing, cuando debió de especificarse el grado de tentativa al entregar el acusado el dinero sustraído del banco.

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1 Apellidos y Nombres: Santisteban Llontop, Pedro

1.2 Cargo e institución donde labora: UCV

1.3 Nombre del instrumento motivo de evaluación: **Guía de análisis de fuente Documental**

1.4 Autor(A) de Instrumento: Zavala Alzamora Karolein Mishel Magdelein
Vigo Baca Luz Benilda

II. ASPECTOS DE VALIDACIÓN:

CRITERIOS	INDICADORES	INACEPTABLE						MINIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. PRESENTACIÓN	Responde a la formalidad de la investigación.												X	
2. OBJETIVIDAD	Esta adecuado a las leyes y principios científicos.												X	
3. ACTUALIDAD	Considera información actualizada, acorde a las necesidades reales de la investigación.												X	
4. INTENCIONALIDAD	Está adecuado para valorar las categorías.												X	
5. COHERENCIA	Existe coherencia entre los objetivos y supuestos jurídicos.												X	
6. METODOLOGÍA	La estrategia responde a una metodología y diseño aplicados para lograr verificar los supuestos.												X	
7. PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al Método Científico.												X	

III. OPINIÓN DE APLICABILIDAD

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

IV. PROMEDIO DE VALORACIÓN:

95 %

Lima, 04 de octubre del 2021

FIRMA DEL EXPERTO INFORMANTE
Pedro Santisteban Llontop
DNI N° 09803311 Tel 983278657

II. ANÁLISIS DE DERECHO COMPARADO

FUENTE	PAÍS	NORMA	IDENTIFICACIÓN DEL OBJETO ANÁLISIS
Código Penal Español https://www.boe.es/buscar/pdf/1995/BOE-A-1995-25444-consolidado.pdf	**ESPAÑA**	**Ley Orgánica 10/1995**	[...] Artículo 248. 1. Cometen estafa los que, con ánimo de lucro, utilizaren engaño bastante para producir error en otro, induciéndolo a realizar un acto de disposición en perjuicio propio o ajeno.
Código Penal Alemán https://perso.unifr.ch/derechopenal/assets/files/legislacion/l_20080616_02.pdf	**ALEMANIA**	**Código Penal Alemán**	[...] 263.a "I. Estafa por computador. Quien, con la intención de procurar para sí o para un tercero una ventaja patrimonial ilícita, perjudique el patrimonio de otro influyendo en el resultado de un proceso de elaboración de datos por medio de una errónea configuración del programa, por medio del uso de datos incorrectos o incompletos, a través del uso no autorizado de datos. [...]
Código Orgânico Integral Penal https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_con_judi_cód_org_int_pen.pdf	**ECUADOR**	**Código Orgánico Integral Penal**	Artículo 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de libertad de uno a tres años.
Ley 19.223 https://derecho.udd.cl/actualidad-juridica/files/2021/01/AJ29_553.pdf	**CHILE**	**Ley 19.223**	*Artículo 2° «El que con el ánimo de apoderarse, usar o conocer indebidamente de la información contenida en un sistema de tratamiento de la misma, lo intercepte, interfiera o acceda a él, será castigado con presidio menor en su grado mínimo a medio».*

Ley Nª 30096 www.gob.pe/institucion/mpfn/informepublicacioness-/1678028-ley-n-30096	**PERÚ**	**Ley Nº 30096**	Artículo 8. Fraude informático El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.
ANÁLISIS DEL CONTENIDO	En ese sentido, se ha podido analizar que, en **España y Ecuador** si existe notorias estrategias para poder implementar un cuerpo normativo que busca lograr un equilibrio jurídico, además se ha introducido en los Códigos Penales de cada legislación el concepto de fraude informático que permite desaparecer gradualmente la ineficacia normativa en la regulación de la modalidad de phishing. **Alemania,** por su parte especifica como medio empleado el computador lo cual en cierta parte ayuda a la regulación de delitos informáticos, pero esto no engloba a todas las modalidades como el phishing que han surgido en los últimos años. Pero**, Chile** y **Perú** acarrean deficiencias en sus leyes de delitos informáticos, pues no se contempló las nuevas modalidades de estos delitos; siendo necesario para la protección del bien jurídico sistematizarlo en el CP, ya que, en la actualidad no se ajusta a la realidad y deben ser sancionados.		

PONDERAMIENTO DE LAS INVESTIGADORAS /CONCLUSIÓN

El análisis de derecho comparado realizado, evidencia la necesidad de modificar la ley incluyendo en forma expresa los delitos informáticos contra el patrimonio, haciendo factible que haya distinciones entre las modalidades, a fin de que se pueda proteger y defender a las víctimas de estos delitos que se desarrollan por un sistema informático como es el caso del phishing.

Ahora bien, **España** ha implementado de forma armónica en el **artículo 248. 1. de la Ley Orgánica 10/1995** la figura de estafa enfatizando los actos que serán materia de sanción; pero, también empleó otras figuras clásicas penales con el fenómeno informático, adoptando la aplicación de leyes especiales con la finalidad de hacer frente al problema de la criminalidad informática.

Asimismo, **Alemania** ha introducido en su legislación el **artículo 263.a del Código Penal Alemán** y complementario a ello usaron nuevos conceptos penales para la represión criminalidad informática, para ello su gobierno tuvo que reflexionar sobre la problemática actual y verificar si la aplicación del Derecho Penal tradicional era suficiente para reprimir esas nuevas acciones que generan nuevos lesiones a bienes jurídicos que era merecedores de protección, aclarando que de nuestra

consideración aún falta indicar y mejorar los medios empleados en estos delitos; ya que, el computador no es la única forma de obtener una ventaja patrimonial en esto casos, por el cual se debe enfatizar las diversas modalidades que han ido surgiendo.

En Ecuador, el artículo 190° del **Código Orgánico Integral Penal**, si bien señala las acciones ilícitas que serán sancionadas, observaremos la carencia en identificar las modalidades en estos delitos informáticos, lo cual sumado a la realidad del país veremos la deficiencia en sus administradores de justicia que va en conjunto a leyes impuestas sin conocerlas.

Por su parte **Chile** no contempla en el **artículo 2° de la Ley Nº 19.223** las nuevas figuras de delitos informáticos como hacking o el fraude informático, de esto modo esto evidencia las falencias en los que incurre su legislación respecto a la regulación de estos delitos, dejando un vacío en la interpretación sobre el significado del sistema de tratamiento de información, sin considerar los medios empleados o especificar adecuadamente la acción punible.

Por último**, Perú** también muestra esas deficiencias en el artículo 8° de la Ley Nº 30096 dado que no permite de forma eficiente imponer un castigo efectivo para los comportamientos ilícitos, ya que en el concepto de fraude informático agrupa todas las posibles modalidades ilícitas sin diferenciarlas y ocasionando ineficacias normativas al emplear la norma o al momento de formulación de la denuncia, generando como efectos el archivamiento, falta de individualización del autor, sobreseimientos por malas aplicaciones en el recojo de la evidencia digital, entre otros.

Objetivo específico 1

Determinar cómo se vulnera la protección a las víctimas de phishing en entidades financieras con la ineficacia normativa, Lima 2020.

III. ANÁLISIS DE INFORME DE ANÁLISIS ESTRATÉGICO

FUENTE DOCUMENTAL	**Informe de análisis estratégico: Denuncias de delitos informáticos investigados por la DIVINDAT 2013-2020** https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUENCIA%20EN%20EL%20PERÚ%20-%20PAUTAS%20PARA%20SU%20INVESTIGACIÓN%20FISCAL%20ESPECIALIZADA%20-%2015%20FEBRERO%202021.pdf
CONTENIDO DE LA FUENTE A ANALIZAR	La División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT), entre 2013 a diciembre de 2020, registró 12 169 delitos vinculados a la Ley N°30096. El 78% (9 515) de los delitos registrados es por fraude informático, seguido por el delito de suplantación de identidad (13%) y delitos contra datos y sistemas informáticos (6%). El delito con mayor cantidad de registros, dentro del fraude informático, corresponde a las operaciones y transferencia electrónicas y/o de fondos no autorizados, con el 86% (8 142). Asimismo, se observa que el registro de los delitos ha tenido un ritmo creciente año a año, donde los registros del 2020 representaron el 134% de crecimiento en comparación a los registros del 2017.
ANÁLISIS DEL CONTENIDO	Las cifras señaladas en el informe de análisis en el contenido de estadísticas oficiales del periodo de octubre de 2013 a diciembre a 2020, muestra el incremento de los delitos informáticos en los últimos años, reflejándose en esta circunstancias de pandemia donde se ha aumentado la incidencia de denuncias de los ciudadanos, además se ha visto múltiples registros de delitos concernientes a la Ley 30096, de los cuales la mayor cantidad corresponde al delito de fraude informático que se efectúa en las operaciones y trasferencias electrónicas. Respecto a las circunstancias las

	denuncias registradas por la División de Delitos de Alta Tecnología ha tenido un ritmo creciente a diferencia de años anteriores.

PONDERAMIENTO DE LAS INVESTIGADORAS / CONCLUSIÓN

El análisis estratégico en el **acápite II de Estadísticas Oficiales del punto 2.1. al 2.3**. elaborado por La División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (DIVINDAT), expone la necesidad de implementar mecanismos eficientes y tecnológicos. Además, se debe tener en cuenta el equipamiento tecnológico necesario, así como el personal capacitado con la finalidad de permitir la lucha eficiente contra estos delitos que son de mera importancia por el grado de incidencia en los que se comete.

Dicho esto, podemos identificar el alto nivel de vulnerabilidad de cualquier ciudadano para ser víctimas de delitos informáticos, con el análisis estratégico observaremos que no existen cifras categorizadas por modalidades de este delito, es decir, no tenemos certeza de la cantidad de víctimas de phishing; resaltando la falta de protección del bien jurídico protegido en estos delitos establecidos en la ley y la ausencia de políticas públicas para proteger legalmente a las víctimas de phishing en entidades financieras, no solo en procesos penales sino también en el fuero administrativo, ya que las leyes nacionales mencionadas en esta fuente no son eficaces teniendo como resultado altos registros de denuncias.

IV. ANÁLISIS DE ARTÍCULO INFORMATIVO EN PÁGINA WEB

FUENTE DOCUMENTAL	Ministerio Público – Fiscalía Superior Especializada en Delitos de Ciberdelincuencia de Lima. https://www.facebook.com/FiscaliaPeru/posts/4034512379964204
CONTENIDO DE LA FUENTE A ANALIZAR	Ministerio Público – Fiscalía Superior Especializada en Delitos de Ciberdelincuencia de Lima. Es importante destacar que la presente fuente documental, fue obtenida de una de las redes sociales con mayor afluencia por las personas y por las instrucciones del estado, esta es Facebook en fecha 17 de junio del año 2021, en la que se está investigando a cargo de fiscal provincial responsable Marcial Páucar Chappa, el primer caso de delitos informáticos que investiga de manera especializada con el equipo de la Fiscalía Superior Especializada en Delitos de Ciberdelincuencia de Lima, recién creada. El caso, en mención señala a una mujer sospechosa de formar parte de una banda criminal, quien a través de la manipulación del sistema informático retiró dinero por el monto de 700 mil dólares, ordenándose inmediatamente su captura y detención preliminar ante el Poder Judicial.
ANÁLISIS DEL CONTENIDO	Lo descrito precisa que, según las primeras indagaciones, la detenida junto otras dos personas integran una banda criminal dedicada a delitos informáticos, primer caso que se ha venido investigando por la nueva Fiscalía Superior Especializada en Delitos de Ciberdelincuencia, lo cual ha rebotado en la red social de Facebook, para evidenciar la actividad que se efectúa y dar con la captura de la imputada.

PONDERAMIENTO DE LAS INVESTIGADORAS / CONCLUSIÓN

Este artículo informativo en página web sobre la **nota informativa** de detención a integrante de banda en primer caso de delito informático con investigación fiscal especializada, muestra que el Estado a través de la normatividad jurídica ha planteado la problemática de los delitos informáticos, creándose la Unidad Especializada en Delitos Informáticos con

propósito de investigar de forma diligente estas figuras delictivas, facilitando la persecución y sanción de las conductas ilícitas que lesionan los sistemas y datos informáticos.

Además, el artículo antes mencionado aprecia el inicio de investigación preliminar a fin de poder individualizar a los sujetos que perpetuaron el ilícito, sin embargo podemos concretar que la víctima de esta modalidad de delito informático hasta el momento no ha podido recuperar su dinero y la entidad bancaria por el cual se efectuó las transferencias no ha realizado ningún pronunciamiento, quedando nuevamente a la deriva la protección a las víctimas de phishing en entidades financieras debido a la existencia de una norma que no es eficaz en su empleo y a pesar de la existencia de la nueva fiscalía aún nos faltaría expresar claramente las modalidades que se pueden presentar del fraude informático para evitar errores con los casos de estafas.

V. ANÁLISIS DE JURISPRUDENCIA INTERNACIONAL

FUENTE DOCUMENTAL	Cámara Nacional de Apelaciones en lo Criminal y Correccional .Sala V. https://jurisprudencia.mpd.gov.ar/Boletines/2016.08.%20Delitos%20informaticos.pdf
CONTENIDO DE LA FUENTE A ANALIZAR	El presente informe ha sido elaborado sobre la decisión de la Cámara Nacional de Apelaciones en lo Criminal y Correccional, que en fecha 24 de octubre del 2013, la Sala V de la Cámara de Apelaciones confirmó el sobreseimiento, señalando que la figura ilícita en materia informática se le conoce como phishing que es empleada por agencias criminales multinacionales para la obtención ilegal de datos secretos, como en el referido cuentas bancarias de terceros, que manipulados de forma remota, permiten el acceso a sistemas informáticos ajenos en los que los sujetos activos logran operar libremente, sacando provecho propio y propiciando un perjuicio a sus verdaderos titulares. Las víctimas de este ilícito han sido sujetos de una misma maniobra delictiva en los que actuaron engañados como simples instrumentos que obraron sin dolo de los auténticos autores del crimen, he aquí lo sustancial para determinar la autoría mediata reside en que el autor no realiza personalmente la acción ejecutiva, sino mediante otro instrumento; por ello, no se ha podido acreditar el elemento subjetivo del tipo penal impuesto.
ANÁLISIS DEL CONTENIDO	La decisión de la Cámara Nacional de Apelaciones en lo Criminal y Correccional establece los lineamientos de autoría y participación, señalando que para plasmar la autoría mediata se da en el caso de utilizar como medio para lograr un fin en concreto, además nos hace mención la exigencia de la actuación del dolo como el instrumento sustancial del ilícito, sino se obraría con error o ignorancia sobre las circunstancias del tipo, de la misma forma de la participación donde el partícipe requiere el conocimiento de la propia acción, es decir tener conocimiento del autor, cosa que los imputados desconocían en su totalidad ya que se realizaron giros de dinero a nombre de terceros en Barcelona.

PONDERAMIENTO DE LAS INVESTIGADORAS / CONCLUSIÓN

La presente jurisprudencia internacional versa sobre la **Causa N°36742/2011. 24/10/2013** en base a la **decisión efectuada por la Cámara Nacional de Apelaciones en lo Criminal y Correccional – Sala V**; que refiere los parámetros de la actuación criminal en defraudación por medios informáticos, como modalidad el phishing, planteando la importancia del dolo en estos actos delictivos realizados en Barcelona.

En consecuencia, debemos tener en cuenta el contexto actual en que vivimos; ya que, esto evidencia el abandono de los administradores de justicia ante el vacío para identificar e individualizar correctamente a los verdaderos autores del delito, siendo esencial la actualización digital. Entonces, según el fallo de la Cámara Nacional de Apelaciones en lo Criminal y Correccional el nivel de participación es distinta si no se tiene conocimiento de los planes del autor, esto incurriría en la falta del dolo como instrumento y no existiría autoría mediata, puesto que en el caso los partícipes actuaron de acuerdo a una simulación de contrato y fueron inducidos a error mediante un engaño para conseguir el apoderamiento patrimonial de forma indebida, perjudicando a los auténticos titulares de las cuentas bancarias (víctimas de phishing) quienes fueron vulnerados en la protección de sus datos, afectándolos económicamente; enfrentándose a una norma que no es eficaz en su empleo, por la falta de identificación del autor que al parecer empleó virus informáticos y contrataciones simuladas de agentes de transferencia de dinero tratándose de una estafa masiva. Si bien concordamos con la decisión tenemos que criticar la ausencia nacional e internacional para obtener justicia para las víctimas de phishing entre otras modalidades, pues los medios y el personal no está capacitado para enfrentar estos casos.

Objetivo específico 2

Identificar la actuación del Ministerio Público sobre la ineficacia normativa para la protección a las víctimas de phishing en entidades financieras, Lima 2020.

VI. ANÁLISIS DE RESOLUCIÓN DE LA FISCALÍA DE LA NACIÓN

FUENTE DOCUMENTAL	Crean la Unidad Fiscal Especializada. https://busquedas.elperuano.pe/normaslegales/crean-la-unidad-fiscal-especializada-en-ciberdelincuencia-de-resolucion-no-1503-2020-mp-fn-1916745-1/
CONTENIDO DE LA FUENTE A ANALIZAR	Crean la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público con competencia nacional y designan y nombran Fiscales en el Distrito Fiscal de Lima. La referida fuente documental, contiene información recabada de una resolución publicada el 30 de diciembre de 2020, en la página web del Diario Oficial del Bicentenario, donde se señaló las funciones de la Unidad Fiscal Especializada en Ciberdelincuencia, que es intervenir en los casos de su competencia y asistir a los fiscales, también recepcionar denuncias y realizar investigaciones preliminares y genéricas, actuar como medio con los diferentes actores e instituciones de ámbito nacional e internacional, además asesorar a los fiscales sobre temas de materia informática, métodos de investigación, obtención, análisis y preservación de la prueba, es así que la creación de la Unidad Fiscal Especializada en Ciberdelincuencia brindará un tratamiento especializado y un acompañamiento técnico a los fiscales en la investigación de los delitos cibernéticos y en la obtención de la prueba digital.
ANÁLISIS DEL CONTENIDO	El precedente informe nos detalla sobre la creación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, debido la evolución de nuevas tecnologías e instrumentos informáticos, la Fiscalía de la Nación dispuso incorporar esta unidad con competencia a nivel nacional.

PONDERAMIENTO DE LAS INVESTIGADORAS / CONCLUSIÓN

La resolución de la **Fiscalía de la Nación N°1503-2020-MP-FN,** según la **parte resolutoria, artículo Tercero,** inciso 6; planteó las funciones que realizaría la Unidad Fiscal Especializada en Ciberdelincuencia; destacando la promoción de articulación de dos entidades tan significativas como el Ministerio Público y la Policía Nacional, teniendo en consideración

el brindar un acompañamiento técnico a los fiscales en la realización de la investigación de los delitos previstos en la Ley de delitos informáticos.

Es así, que consideramos importante esta actuación del Ministerio Público; ya que, consolida los criterios planteados en los procedimientos y métodos de investigación en materia de ciberdelincuencia buscando orientar a los fiscales penales en la realización de investigación dando frente a la ineficacia normativa, falta de políticas públicas, mala interpretación de la norma. También trata de vincular como en otros países se ha ido ejecutando y ha funcionado cabalmente ante la lucha de los nuevos delitos informáticos, recordando que el principio de cooperación efectuado entre los países debe emplearse congruentemente con el manejo de cada ministerio buscando unanimidad para obtener un empleo de justicia eficiente en diversas materias legales.

VII. ANÁLISIS DE JURISPRUDENCIA INTERNACIONAL

FUENTE DOCUMENTAL	Convención de Budapest contra la ciberdelincuencia https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
CONTENIDO DE LA FUENTE A ANALIZAR	La presente convención fue firmado el 21 de noviembre del 2001, este convenio fue uno de las principales y más completos en la cooperación internacional, se sustentó en armonizar las figuras de los delitos basado al derecho sustantivo penal de cada país y las disposiciones conexas en relación a delitos informáticos, de esta manera estableció mediante el derecho procesal penal los mecanismos sustanciales para la investigación y procesamiento de dichas contravenciones, así como también de los delitos cometidos a través del sistema informático, garantizando un régimen rápido y eficaz de cooperación internacional. Plasmando en su artículo 8, el concepto de fraude informático: " Las partes adoptarán las medidas legislativas […] [*de*] actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a. la introducción, alteración, borrado o supresión de datos informáticos […]" .
ANÁLISIS DEL CONTENIDO	Este convenio por su carácter de operacionalidad ha constituido en uno de los más principales esfuerzos para hacer lucha a la cibercriminalidad, es sin duda un esfuerzo internacional donde varios países están unidos para asumir la responsabilidad de reconocer la importancia de imponer sanciones y mecanismos efectivos de investigación, que sean adecuados y dinámicos para hacer frente a estos comportamientos delincuenciales en favor de una sociedad que tiene un desarrollo tecnológico. Siendo así, que estableció las pautas de colaboración, supervisión y mutua coordinación entre distintas legislaciones con el único fin de evitar la evasión de la persecución penal conforme lo establecido en el artículo 8 concerniente a fraude informático, el cual englobaría las diversas modalidades entre ellas, el phishing.

PONDERAMIENTO DE LAS INVESTIGADORAS / CONCLUSIÓN

La jurisprudencia internacional hace mención al **artículo 8° del Convenio de Budapest**; el cual define los delitos informáticos como la acción de introducir, alterar, borrar o suprimir datos de esta índole, agregando cualquier interrupción en un sistema informático.

Se debe precisar que en general el convenio conceptualiza al sistema informático como cualquier dispositivo aislado o grupo de dispositivos conectados o relacionados entre sí, cuya función de cualquiera de sus elementos es el procesamiento automático de los datos de ejecución del programa. Por ende, para buscar una definición sobre los delitos informáticos se