



FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

Carrera de Derecho y Ciencias Políticas

“LA TIPIFICACIÓN DEL PHISHING, SMISHING Y VISHING EN NUESTRO SISTEMA PENAL PERUANO, PARA LA LUCHA CONTRA LA CIBERDELINCUENCIA EN LIMA, 2020”

Tesis para optar el título profesional de:

Abogada

Autora:

Mishell Alisson Ventura Quijano

Asesor:

Dr. Gregorio Wilfredo Roque Ventura

Lima - Perú

2021

DEDICATORIA

La presente tesis está dedicada primero a Dios por darme la fortaleza de seguir adelante cada día frente a las adversidades, ser mi guía ante las dificultades y hacerme entender que la razón vital del ser humano en la tierra es encontrar la felicidad de todas las formas posibles.

También está dedicada a mi padre Yonel Ventura Tacuche, a mi madre Flor María Quijano Candelario y a mi hermano Steevem Ventura Quijano, quienes a lo largo de mi vida siempre inculcaron en mí valores como la perseverancia, no solo para ser una excelente profesional, si no para ser un miembro integro para sociedad. Cada uno de mis objetivos y anhelos no serían posibles sin la ayuda de ellos.

Mishell Alisson Ventura Quijano

AGRADECIMIENTO

Debo expresar mi gratitud primero a la Universidad Privada del Norte, mi casa de estudios quien me brinda muchas oportunidades para seguir adelante, también a mis profesores que durante la carrera inculcaron en mí la pasión por el Derecho, además de haber descubierto que la integridad es la base de todo ser humano.

También quiero hacer un agradecimiento especial a mi familia quien es mi inspiración para cada paso que doy, lo único que deseo en esta vida es siempre hacerlos sentir orgullosos de mí, no solo por la calidad de profesional que debo ser, sino por los valores inculcados durante mi corta vida.

Y, por último, agradecer a mi asesor de tesis el Dr. Gregorio Wilfredo Roque Ventura que me acompañó en esta corta pero enriquecedora etapa, debo mencionar mi profunda admiración, por su inteligencia que denota en sus palabras, le deseo todo lo mejor.

ÍNDICE

DEDICATORIA	2
AGRADECIMIENTO.....	3
ÍNDICE DE TABLAS	5
ÍNDICE DE FIGURAS	6
RESUMEN	7
ABSTRACT	8
CAPÍTULO I. INTRODUCCIÓN	9
1.1. Realidad Problemática	9
1.3. Objetivos	25
1.4. Hipótesis.....	25
CAPÍTULO II. MÉTODO.....	27
2.1 Tipo de Investigación.....	27
2.2 Población y muestra (Materiales/Instrumentos).....	27
2.3 Operacionalización de variables.....	29
2.4 Técnicas e instrumentos de recolección y análisis de datos.....	30
2.5 Procedimiento	32
2.6 Aspectos éticos.....	33
CAPÍTULO III. RESULTADOS	34
3.1 Resultados de análisis documental.....	34
3.2 Análisis documental del Poder Judicial	40
3.3 Resultado del análisis de las entrevistas.....	45
3.4 Resultados del análisis de la legislación	57
CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES	64
4.1 Discusiones	64
4.2 Conclusión.....	77
4.3 Recomendación	78
REFERENCIAS	82
ANEXOS	87

ÍNDICE DE TABLAS

Tabla 1	29
Tabla 2	31
Tabla 3	31
Tabla 4	58
Tabla 5	59
Tabla 6	61
Tabla 7	62
Tabla 8	71

ÍNDICE DE FIGURAS

Figura 1	34
Figura 2	35
Figura 3	36
Figura 4	37
Figura 5	38
Figura 6	39
Figura 7	40
Figura 8	41
Figura 9	42
Figura 10	43
Figura 11	44
Figura 12	45

RESUMEN

La criminalidad informática o la ciberdelincuencia es un delito realizado mediante la utilización de medios tecnológicos. Estas conductas se materializan principalmente con la obtención de datos informáticos, suplantación de la identidad, vulneración al secreto a las comunicaciones y la interceptación de datos informáticos o fraude informático. De ahí nace la importancia de crear mecanismos para proteger el sistema informático creando seguridad informática. Por otro lado, gracias a la globalización, muchas personas se han beneficiado adoptando el e-commerce “comercialización y venta de productos a través de medios electrónicos”, y con ello yace la necesidad de proteger aquellas actividades económicas que se realizan por medios digitales. Es por ello que entró en vigencia la Ley de delitos Informáticos n.º 30096 y su modificatoria la Ley n.º 30171. A partir de este momento la ley adquirió mayor relevancia, ya que tiene como objetivo primordial la protección de bienes jurídicos. Para su elaboración nuestros legisladores utilizaron bases internacionales como el convenio de Budapest, convenio creado para hacer frente a los delitos informáticos a través de mecanismos de homologación de normas de derecho penal sustantivo. No obstante, el Perú recién en el año 2019 incorporó su tratamiento mediante resolución Legislativa n.º 30913 y fue ratificado mediante Decreto Supremo n.º 010-2019-RE. Esta deficiencia legal nos llevó a que durante muchos años se cometan fraudes cibernéticos sin que se tomen medidas acordes a la importancia requerida. El objetivo de este trabajo es implementar las modalidades como el *phishing*, *smishing* y *vishing* como delitos penalizables en nuestro sistema penal, reforzar mecanismos ya existentes para la prevención de los delitos cibernéticos y la importancia de adquirir una educación en seguridad informática en el Perú, nuestra realidad social hoy en día nos ha hecho ver que tenemos deficiencias legales para el tratamientos de los delitos informáticos y su aplicación, la falta especializaciones con respeto al proceso legal para la imputación del delito, la carencia de medios tecnológicos para facilitar el trabajo de los fiscales y sobre todo la imposibilidad para identificar el perpetuador del daño.

Palabras clave: (Informática, Ciberdelincuencia, incorporación, delito, penalización e-commerce).

ABSTRACT

Computer crime or cybercrime is a crime carried out through the use of technological means. These behaviors mainly materialize with the obtaining of computer data, identity theft, violation of communications secrecy, interception of computer data or computer fraud; hence the importance of creating mechanisms to protect the computer system by creating computer security. On the other hand, thanks to globalization, many people have benefited by adopting e-commerce "commercialization and sale of products through electronic means", and with this lies the need to protect those economic activities that are carried out by digital means. This is why the Computer Crimes Law n°. 30096 and its amendment Law n°. 3017 came into force, from this moment the law acquired greater relevance, since its primary objective is the protection of legal assets, for its preparation our legislators used international bases such as the Budapest Convention, an agreement created to deal with computer crimes through mechanisms of homologation of substantive criminal law standards; However, Peru only in 2019 incorporated its treatment through Legislative Resolution n°. 30913 and it was ratified by Supreme Decree No. 010-2019-RE, this legal deficiency led us to commit cyber fraud for many years without the required importance. The objective of this work is to implement modalities such as phishing, smishing and vishing as criminal offenses in our penal system, reinforce existing mechanisms for the prevention of cybercrimes and the importance of acquiring an education in computer security in Peru, our Today's social reality has made us see that we have legal deficiencies for the treatment of computer crimes and their application, the lack of specializations with respect to the legal process for the imputation of the crime, the lack of technological means to facilitate the work of prosecutors and above all the impossibility to identify the perpetrator of the damage.

Keywords: (IT, Cybercrime, incorporation, crime, electronic commerce penalty).

CAPÍTULO I. INTRODUCCIÓN

1.1. Realidad Problemática

1.1.1 Presentación y descripción del problema

El presente trabajo se sitúa en el ámbito de las nuevas modalidades emergentes para la comisión de delitos informáticos. Esta investigación tiene como objetivo primordial justificar por qué los delitos como el phishing, que consiste principalmente en la utilización de suplantación de páginas webs, *smishing*, que consiste especialmente en la utilización de mensajes de texto, y *vishing*, que consiste en esencia en la utilización de llamadas por medios tecnológicos, deben ser tipificados en legislación penal del Perú. Para ello, deben ser incluidos en la Ley n.º 30096 y su modificatoria Ley n.º 30171, así como una debida penalización de estos delitos. En este sentido, debemos tener en cuenta que la implementación de estas modalidades de comisión de fraudes informáticos servirá para mitigar la comisión de los delitos informáticos, y lograr identificar el espacio virtual donde se computan dichos ilícitos; ya que debido a su naturaleza exige que los agentes de justicia se encuentren meramente calificados para su tratamiento. Para ello, deberían realizar especializaciones para distinguir las diferentes modalidades mediante las cuales se comisionan estos ilícitos penales, de modo tal que se rompa con aquellas directrices habituales para la imputación de un delito tradicional.

Además, el objetivo de este trabajo está orientado a justificar la importancia de la incorporación de las nuevas modalidades de comisión de fraudes informáticos, como es el caso del phishing, smishing y vishing en la legislación penal. Esto a su vez ayudaría a la delimitación del tratamiento del Art 8 de la Ley n.º 30096, el cual consideramos que el Perú debió recoger luego de la adhesión al convenio de Budapest, que entró en vigor el 1 diciembre 2019, y que contribuiría a hacer frente a la ola discriminada de estos delitos que sufre el Perú. Esta ola es consecuencia no solo de la deficiente capacidad de respuesta que hoy en día tienen los agentes que imparten justicia, sino también por la falta de capacitación que en estos casos se requieren por su naturaleza. Además, mediante el desarrollo del trabajo podremos observar que la tasa de denuncias ha tenido un auge considerable sobre todo en el periodo del 2019 y 2020. Por otra parte, también podremos darnos cuenta que en muchos casos la falta de peritos en materia tecnológica, lo que resulta ser deficiente; circunstancia que ha conllevado a la dificultad para lograr

identificar y sancionar a los autores del delito, generándose así la falta de seguridad jurídica.

En la actualidad las conductas perpetradas mediante medios tecnológicos, ya por su complejidad o modalidad empleada, muchas veces resultan ser incapaces de ser reprimidas con los dispositivos penales tradicionales. En ese sentido, mediante el presente trabajo se pretende demostrar que es imprescindible que las modalidades como el *phishing*, *smishing* y *vishing* estén reguladas y penalizadas dentro del ámbito de fraude informático como una categorización de ella, para hacer frente así a la ciberdelincuencia en el Perú.

1.1.2. Antecedentes de la investigación

1.1.2.1. Antecedentes Internacionales

Uno de los convenios europeos sobre ciberdelincuencia, conocido como convenio de Budapest, es uno de los primeros acuerdos internacionales adheridos por parte del Perú con la finalidad de hacer frente a la ciberdelincuencia, su proceso de implementación y su impacto sociológico. Una de las características que propone dicho convenio es la disposición e interceptación de datos. De la misma forma Chocobar (2019), secretaria de gobierno digital, nos señala que es importante que el Perú invierta en seguridad digital para formar así una cultura de ciberseguridad y defensa digital, para evitar que muchos usuarios sean vulnerables ante eventuales ataques informáticos, realizando así inversiones a nivel de empresas privadas o empresas del estado.

En referencia Barboza (2018), nos habla que la tecnología ha generado mecanismos que facilitan el uso de dinero virtual, como tarjetas de crédito, y como resultado estas nuevas formas de comercio han abierto paso a la criminalidad informática, una de las principales problemáticas en Colombia es el fraude electrónico a partir del uso de tarjetas de crédito el cual es uno de los principales problemas del sistema financiero, el fraude electrónico también es cometido a través del *phishing* y *vishing*, este tipo de modalidad es cometido mediante la falsificación de portales web que intentan acceder a la información de las tarjetas de crédito, mientras que el caso del *vishing* este delito se comete a través del llamado telefónico suplantando personal de las entidades bancarias para incurrir en error a los usuarios de tal forma les proporcione información confidencial de manera indirecta.

Hasta este momento podemos destacar que tanto países como de América latina son las principales víctimas de estas nuevas modalidades de comisión de delitos informáticos como el *phishing*, *vishing* y *smishing*. Estas generan una afectación al sistema financiero por medio de la suplantación de identidad, al incurrir en error al usuario para así robarle información. Una de las problemáticas, tal como explica el autor, es que no solo basta con que se enriquezcan de material jurídico, si no también que inviertan en seguridad informática y una adecuada implementación de la norma, es decir la actualización del marco jurídico; ya que la persecución de los delitos informáticos es más compleja que los delitos tradiciones porque requiere necesariamente reunir todos elementos sustanciales para su imputación.

Acurio (2018), en su artículo, explica que las maniobras para la comisión de delitos informáticos comprenden la manipulación que tiene como finalidad lograr movimientos falsos. Este delito es uno de los más comunes. Entre otro tipo de modalidades tenemos la técnica de salami, *phishing*, esta última se encuentra diseñada con la finalidad de robarle la identidad del usuario obteniendo información privada que es usada por medio de engaños, utilizando ventanas emergentes o mensajes de los correos electrónicos. En otras palabras, el del *phishing* tiene como objeto buscar grupos vulnerables para inducirlas en error.

De acuerdo con Rodríguez (2019), una de las aproximaciones del *phishing*, es que es una de las formas más clásicas de comisión de ilícitos penales, que con ánimo de lucro utilizan el engaño para inducir en error al usuario y provocar un perjuicio económico. El consejo de la Unión Europea adoptó medidas para garantizar que esas conductas sean delitos penales. El ánimo de lucro y la manipulación informática son cometidos mediante el uso de medios tecnológicos, y es concretada mediante una transferencia no consentida. La defraudación económica es parte de la manipulación informática. Es por el ello que el tribunal considera la manipulación del hardware-software¹ que se computa para introducir datos. El *phishing* es cometido mediante un agente que se denomina mulero, cuya función es almacenar y transmitir dinero fruto de la manipulación informática.

¹ Hardware: Es el conjunto de componentes físicos de los que está hecho el equipo.

Software: Es el conjunto de programas o aplicaciones, instrucciones y reglas informáticas que hacen posible el funcionamiento del equipo.

En relación a esto, Salazar (2019), menciona que la evolución ha influenciado en nuevos medios tecnológicos para obtener información y darle seguridad al mundo virtual. El comercio en línea es un espacio que plantea problemáticas sobre seguridad, ya que al realizar cualquier transacción financiera o pago electrónico se puede ser víctima de un fraude cibernético. El modus operandi de los ciberdelincuentes es usar técnicas de persuasión. Las modalidades más usadas son el *phishing*, *smishing* y *vishing* debido a la acogida que tiene en el comercio electrónico. Estas consisten en el hurto de información personal, a través de los denominados “ladrones del phishers”, para atacar a sus víctimas por medio del correo electrónico, solicitando datos personales. Entonces, cuando el usuario entra al correo electrónico, sin darse cuenta proporciona datos personales y es así como se convierte en una víctima del *phishing*. Existe dos clases de phishing: el tradicional y el complejo. El primero se envía de forma masiva a correos electrónicos escogidos a la suerte, Lo primordial es identificar este tipo de fraude mediante detalles importantes, el primero de los cuales es verificar la dirección del URL² y el “https://. De este modo se logra evitar ser víctimas de la ciberdelincuencia.

Espinoza (2017), nos habla que la informatización de la sociedad es por la influencia de la tecnología del TIC “Tecnologías de la información y la comunicación”. El tratamiento de información jurídica necesaria como el software, gestión de leyes, doctrina y jurisprudencia, la comunidad ha conseguido una relación entre la ciencia del derecho. El derecho penal informático estaría previsto en los datos necesarios para plantear soluciones normativas para la reducción de la ciberdelincuencia, dado que el objetivo es que mediante la interpretación de las leyes penales sobre delitos informáticos se reduzcan las modalidades para su comisión. Lo que se propone es la reducción de los delitos informáticos para el control de la sociedad frente al mundo digital y darles seguridad jurídica a las leyes sobre delitos informáticos, con el fin de reducir los índices de cibercriminalidad. El delito informático es aquella conducta que daña bienes jurídicos relacionados con la tecnología, como una conducta típica, antijurídica y culpable cuyo objeto es la protección de tecnología de información.

² URL o Localizador Uniforme de Recursos, es la dirección específica que se asigna a cada uno de los recursos disponibles en la red con la finalidad de que estos puedan ser localizados o identificados.

1.1.2.2. Antecedentes Nacionales

Para comenzar, una de las problemáticas en el Perú, es el auge de la ciberdelincuencia vinculado al desarrollo económico. Cada vez nuestra vida gira alrededor de actividades más digitalizadas; las políticas sobre ciberseguridad son importantes para salvaguardar bienes jurídicos protegidos en el ámbito digital, y uno de los grandes retos es poder generar seguridad informática para que los usuarios pueden acceder a dichas tecnologías sin convertirse en víctimas potenciales. En tal sentido, Schwartz (2020), nos señala que los daños económicos por ataques cibernéticos sobrepasan el 1% del PIB, de modo que los medios tecnológicos generan oportunidades para que los ciberdelincuentes cometan delitos en el mundo digital.

Es por ello que una de las estrategias por las que optó el Perú para la lucha contra la ciberdelincuencia fue la adhesión al convenio de Budapest a través de la resolución Legislativa n.º 30913, publicada el 13 de febrero 2019. De acuerdo a la ONU (2020), ya existen 12 países que habían aprobado estrategias nacionales sobre ciberseguridad. Uno de los objetivos de este convenio se basa en la capacidad nacional de los países para prevenir delitos cibernéticos, para contrarrestar así las amenazas cibernéticas es necesario que los países cuenten con políticas, legislación y capacitaciones.

Mientras tanto Garrido (2019), afirma que existe una necesidad de incorporar los delitos del *phishing* y *pharming* como modalidades que se realizan a través del sistema informático, el cual vulnera derechos informáticos. Si bien es cierto que la tecnología representa un medio que proporciona facilidades a diversas actividades, está también puede ser usada con un fin malicioso para obtener provecho económico, y la imposibilidad de imputabilidad de delitos generan inseguridad jurídica para aquellos actos que la norma no regula. Una de las características para la comisión de las defraudaciones es la sensación de miedo para someter a sus víctimas al engaño y así robarle información personal.

Por consiguiente, una de las razones mediante la cual los legisladores deben realizar un análisis sobre la incorporación de estas nuevas modalidades, es reconocer la necesidad evidenciada en el aumento de denuncias en los últimos años. De acuerdo con Flores (2018), Perú es el quinto país de Latinoamérica en sufrir la mayor cantidad de ataques cibernéticos, y sobre ello los grupos más afectados son el sector financiero. Siendo así,

la mayor necesidad en el Perú hoy en día es idear mecanismos que contrarresten el gran número de ataques cibernéticos y así proporcionar seguridad informática.

Asimismo, Avalos (2020) hace referencia a que el Perú debe considerar la importancia de una adecuada especialización fiscal para sus servidores públicos, y la necesidad de la construcción de elementos para la imputación de los delitos informáticos como parte de una política institucional efectiva. En definitiva, existe una gran diversidad de delitos, pero estos no hacen referencia a la problemática social. Sin embargo, estas deben ser enumeradas; el uso de la tecnología podría establecer indicadores para la obtención de la prueba digital, de modo que estas serían determinantes para la investigación.

Sin duda alguna cabe mencionar la ardua labor que realizan las unidades especializadas a pesar de no contar con medios tecnológicos innovadores y la cooperación directa con las entidades para combatir los delitos informáticos y hacerlos frentes ante una realidad social inminente como el incremento de denuncias sobre esta problemática. Tal como lo señala la división de investigación de delitos de alta tecnología de la Policía Nacional del Perú “DIVINDAT”, entre el 2013 y 2020 se registraron aproximadamente 12 169 denuncias vinculadas a la Ley n.º 30096. Casi en su mayoría, el 78% de los delitos cometidos son por fraudes informáticos, y su incidencia se sitúa en la ciudad de Lima. A propósito de esto, muchos de los fiscales sostienen que las investigaciones de estos delitos recaen en la etapa preliminar por falta de obtención de información por medios tecnológicos.

En la misma línea, Vílchez (2020) nos habla que a consecuencia de la crisis de salubridad que sufrió cada país del mundo durante la pandemia del COVID-19, muchas de las relaciones sociales y económicas se han desarrollado por el empleo de medios tecnológicos, los que han propiciado la ciberdelincuencia y han dejado al descubierto las dificultades de investigación y el enjuiciamiento de la ciberdelincuencia, la falta de capacitación policial y el uso de técnicas especializadas. Ha quedado en evidencia la necesidad de clasificar algunos criterios normativos para mejorar su tratamiento en un proceso penal y la incorporación de nuevas figuras delictivas.

En conclusión, una de las prioridades del sistema judicial penal es poder subsanar las deficiencias legales que existen en el Perú para poder lograr identificar a los autores de la comisión de los delitos cibernéticos y la dificultad de los cortos plazos de investigación. Tal como lo señala Zevallos (2020), uno de los retos para que el Perú realice una transformación digital conlleva a hacer una reflexión ante amenazas sobre la vulneración

de seguridad informática; es necesario la protección de infraestructura de la información y establecer la conformación de un consejo sobre ciberseguridad, con el objetivo de generar una gestión en riesgos informáticos; así como, consecutivamente, la colaboración de información tanto en sectores públicos y privados necesaria para denunciar ataques cibernéticos y brindar a los usuarios estabilidad informática.

1.1.3. Bases Teóricas

Evolución histórica de la criminalidad informática

La revolución industrial y la nueva era del ciberespacio nos ha mostrado la existencia de diversas formas de comunicación, ya sea por aplicaciones o las redes sociales que han facilitado la interacción humana. En 1969 nadie esperaba que fuera el inicio de una nueva era, que nos ha abierto infinidad de facilidades para actividades cotidianas e incluso sociales.

Por consiguiente, el impacto que ha ocasionado la digitalización ha generado que nuestra realidad y sociedad cambie, y con ella la forma tradicional que teníamos de realizar actividades cotidianas. Como resultado, las nuevas modalidades de comisión de delitos y su perpetuación, incluso nuestra nueva realidad, ha dado lugar a nuevas figuras delictivas que hasta donde sabíamos eran completamente desconocidas para nuestra sociedad.

Un hito importante fue la creación de ARPA net³, creada por Estados Unidos, y a comienzo de los años 70s, Robert Kahn y Vinton Cerf desarrollaron un nuevo prototipo de comunicación destinado a la transmisión de información entre redes. La internalización de esta y el uso comercial que se le dio, hasta el día de hoy hace difícil localizar e identificar al perpetrador, produciendo un daño de manera rápido e irreversible ya que debido a la expansión de la red esta no es borrada en su totalidad. El daño a la información aún sigue siendo complejo, pues el ciberespacio es un mundo digital que cada día se va expandiendo y con ello nuevas formas de cometer delitos, vulnerando derechos que a medida del tiempo estas se han ido externalizando de manera física y emocional (Zabala,2008).

³ ARPA net: Red de Agencias de Proyectos de Investigación Avanzada, red de computadoras construida para enviar datos militares y conectar principales grupos de investigación a través de los Estados Unidos.

Convenio de Budapest en el Perú

El convenio de Budapest es un tratado Internacional iniciado por países miembros del Consejo Europeo y ratificado en noviembre del 2001 en la ciudad de Hungría. Está suscrito por 56 países y en la actualidad muchos de los países de América Latina aún siguen incorporándolo a su legislación con la finalidad de mitigar los daños que ocasionan los delitos informáticos “Dirección de la academia de la Magistratura del Perú, 2019”.

Posteriormente, en la actualidad, los delitos informáticos se encuentran establecidos en Capítulo X del Código Penal y ratificados en la Ley n.º 30171 “Ley que modifica el n.º 30096 ley de delitos informáticos”, con la finalidad de crear estándares sobre criminalidad. Uno de los aspectos que se analizó es la similitud de la redacción con el convenio de Budapest, puesto que lo que se busca es crear mecanismos de homologación de formas de derecho penal y cooperación nacional.

La era tecnológica se ha transformado en medio masivo de interacción entre usuarios, donde se caracteriza por la delgada brecha entre el mundo virtual y la realidad física. La evolución tecnológica se concreta al promover muchas posibilidades de beneficio tanto como a grupos empresariales o entidades que buscan informar nuevos usos científicos, sociales y hasta de entretenimiento. No obstante, las diferentes formas de comercialización virtual, el uso de dinero digital se ha externalizado a campos virtuales que hoy en día es difícil poder configurar (Bollina,2008)

El convenio de Budapest se creó con la intención de realizar una estrategia para proteger el sistema digital. Los delitos informáticos buscan crear un marco penal común y la persecución penal. Una de las características del convenio de Budapest es que sus directrices están orientadas a la integración a todos los países miembros y la obligación de que los países miembros de este convenio transen información entre sí. La masificación del internet provocó mejorar las condiciones de protección de derechos y la regulación sobre el comercio virtual; es por ello la creación de mecanismos que aseguren su protección como normas estandarizadas de los procesos informáticos como Instituto Nacional de Calidad (INACAL) y la División de Delitos de Alta tecnología de la Policía Nacional (DIVINDAT) de modo así asegurar la protección de derechos de los usuarios que son víctimas de delitos informáticos.

Realizado por ciberseguridad del Inter-American Development Bank (2020).
Ciberseguridad riesgos y avances y el camino a seguir América Latina y el Caribe.

En Perú existe la necesidad de realizar una estrategia nacional de seguridad cibernética. Su ausencia hace deficiente la aplicación para salvaguardar los derechos fundamentales y las malas prácticas con respeto a infraestructura. Podemos analizar que la aplicación efectiva por parte de los operadores justicia, la falta de existencia pública disponible sobre la incurrancia de este tipo de delitos y la tarea difícil de llegar a formalizarlos dentro de un proceso penal y sobre todo la carencia de acumulación de pruebas que permiten demostrar la comisión de delitos informáticos.

Definición de Delitos informáticos

Para la realización de la investigación es importante definir conceptualmente el significado de delitos informáticos en el campo jurídico; un término muy usado ante conductas donde intervienen el uso de tecnología que afecten diferentes tipos de bienes jurídicos. Por otro lado, muchos delitos se han ejecutado a través de esta modalidad sin afectar el principio de legalidad, los delitos informáticos se encuentran regulados en el Art186, inciso3, Código Penal de 1991. No obstante, la tipificación no estaba suscrita como un delito autónomo, si no como una agravante del delito de hurto. Eventualmente, estas se encuentran previstas en el Capítulo X del Código Penal y la incorporación de leyes especiales como la Ley n.º 30096 “ley de delitos informáticos” y su modificatorias Ley n.º 30171. Esta última tiene como finalidad adecuar los estándares del Convenio de Budapest sobre la cibercriminalidad incorporados en el art 2.3.4.7 y 10. Uno de los aspectos procesales es establecer garantías a la incorporación del convenio. Una de las singularidades es la Cooperación Judicial Internacional, tipificada en el libro VII.

Asimismo, muchos autores señalan que la cibercriminalidad es un medio tecnológico para concretar el delito, tal como lo señala Curio (2016) en su libro nos habla acerca que las nuevas manifestaciones de las tecnologías de información han surgido comportamientos valiosos y la difícil tarea de la tipificación en las normas penales y la imputación de ellas, la valorización de operadores de justicia para identificar si se trata de un bien económico o hablamos de netamente de bienes jurídicos constitucionales.

Esto se puede definir como la realización de la acción que es llevado a cabo mediante la utilización de medios informáticos que posibilitan la comisión específica de estos delitos vulnerando así un elemento informático como el Software o Hardware, por consiguiente, esta se concreta mediante la acción típica, antijurídica o culpable.

Santiago Curio del Pino nos habla de la existencia de una pluralidad de modalidades delictivas y la multiplicidad, las formas de comisión de delitos informáticos se computan siempre en cuando la utilización esté relacionada con medios tecnológicos, mediante el cual la víctima ha sufrido una pérdida.

- **Sujeto activo**

De acuerdo con Altamirano (2010), el sujeto es la persona individual con capacidad penal que realiza la conducta típica. Solamente una persona individual puede cometer delitos. En este caso podríamos advertir que el sujeto activo es cualquier persona humana capaz que tenga dominio conocimiento en tecnología informática para cometer un hecho punible. Aun en los casos de asociación criminal, las penas recaen solo en sus miembros integrantes.

- **Sujeto pasivo**

El sujeto pasivo por el contrario hace referencia a aquel que ha sufrido la vulneración de un bien jurídico tutelado o puesto en peligro, mediante el cual recae responsabilidad penal. Se describe como aquel que realiza la conducta típica de un hecho punible y reprochable como parte de la individualidad de la pena Por otro lado, es el titular del interés jurídico lesionado o puesto en peligro.

Delitos de peligro abstractos

Los delitos de peligro abstracto se refieren a la relativa carga de la ofensividad mínimo del injusto penal, de la teoría de la imputación objetiva; es decir, a la peligrosidad como mero motivo para legislar, y la persecución de la conducta del peligro del bien jurídico. Una de las características de los delitos de peligro abstracto es que el fin de las prohibiciones penales tiene como residencia evitar los peligros de los bienes jurídicos. Estas se dan sin ninguna prohibición ni relación con la posibilidad real de afectar un bien jurídico y el castigo materialmente de conductas no peligrosas pero coincidentes con el tipo, el comportamiento de acciones que no vulneran los bienes jurídicos a fin de evitar posteriormente una lesión. En otras palabras, se trata de conductas que no producen un peligro concreto, si no que ante una aproximación de ellas ya carece de la aptitud de lesionar un bien jurídico, y esto se adecua para lesionar algún interés meramente individual. A su vez Bajés (2020) menciona que:

Los delitos de peligro abstracto protegen bienes jurídicos supraindividuales, como la seguridad vial, la salud pública, el medio ambiente. Estos bienes se caracterizan por la circunstancia de no pertenecer a un titular individual y determinado, sino al conjunto de la sociedad. Pero como decía estimar los tipos que protegen estos intereses se estructuran como delitos de peligro abstracto implica entender que los mismos disponen de un referente individual potencialmente lesionado por la conducta (p.119)

No obstante, el valor de supraindividual protegido tiene una carencia individual de modo que la consumación se produce con la lesión del mismo puesto que la lesión recaería en el tipo penal de un interés supraindividual para proteger un interés individual. Para esto, Vallejo (2018) menciona que:

A pesar de que es habitual recurrir a la técnica del peligro abstracto para la protección de intereses supraindividuales, lo cierto es que la misma también se utiliza para la tutela de bienes individuales este tipo de delito se consuma con la realización de la conducta desaprobada, sin que sea necesario además lesionar la fama o la propia estimación de la víctima (p,284)

De modo que la individualidad de los bienes jurídicos penales supraindividuales recae en la estructura del tipo objetivo de peligro abstracto consumados de la tentativa de la imputación objetiva de la relación de la conducta capaz de lesionar un bien jurídico penal individual. Una de las problemáticas de los delitos de peligro abstracto es que si este puede criminalizar la conducta contradiciendo la antijuricidad formal y si es necesario que este afecte a un bien jurídico protegido.

La figura de los delitos de abstracto surge de castigar ciertas conductas, ya que llevan consigo el peligro de un bien jurídico a diferencia de los delitos de peligro concreto, que el peligro nace de bien jurídico como elemento del tipo de modo que este se consuma cuando se ha producido realmente el peligro de un bien jurídico desde un punto dogmático. Los delitos de peligro concreto son delitos de resultado, tal como lo señala Bajés (2020):

Los delitos de peligro abstracto contra bienes jurídicos supraindividuales, la conducta disponga de un grado de injusto suficiente como para ser compatible con los principios de lesividad y proporcionalidad, consistente en evitar la realización de conductas que aparezcan en el momento de emprenderse como objetivamente peligrosas para los intereses que la comunidad ha identificado como más esenciales (p,257)

Tal peligrosidad puede ser tácita, sobreentendida de modo general o estadístico. En esa clase de conducta; en tales delitos un sector sostiene que hay una presunción iuris et de iure de peligro que no admite prueba en contrario y considera por ello delito de peligro hipotético; pero otro sector considera que el principio de ofensividad requiere que en esta clase de tipo la presunción de peligro sea iuris tantum, es decir, que admita la prueba en contrario en el caso concreto. O bien la peligrosidad es expresa, requerida explícitamente por la descripción legal, que exige idoneidad de la conducta para lesionar.

Bienes jurídicos supraindividuales

Los bienes jurídicos supraindividuales se refieren al objeto de protección de la doctrina delimitando el objeto material del delito. El derecho penal protege bienes jurídicos personales, pero también de patrimonio donde se incluye los llamados intereses difusos. Estas son realidades valoradas socialmente que afectan a diversas personas sin que estas se encuentren encarnadas en objetos tangibles. Paralelamente, Sánchez (2018) menciona:

Los bienes jurídicos supraindividuales de un referente individual, se asegura que la conducta penalmente relevante tenga un grado de nocividad social suficiente, al caracterizarse la misma por su carácter perturbador para la convivencia colectivo.

Los delitos de peligro abstracto contra bienes jurídicos supraindividuales se enmarcan en que no es necesario esperar la lesión de un bien jurídico individual para la relación del tipo penal. Los bienes jurídicos supraindividuales tienen como característica castigar conductas de actos inofensivos desde la visión de la libertad individual como es el caso de los ilícitos penales del *phishing*, *smishing* y *vishing* cuya protección recae en la seguridad informática.

Seguridad Informática

Para comenzar, el termino de seguridad informática es la conformación de los pilares de la ciencia tiene un arraigo de proporcionar bienestar digital a los usuarios. Muchos de los países Euroasiáticos consideran que la seguridad informática está ligada a la soberanía nacional, encargada de las técnicas y métodos que buscan almacenar información. Una de las características es mitigar los riesgos que provocan el extenso mundo a la información digital y la entrada de datos por medio del hardware. Uno de los propósitos de la seguridad informática es proteger la información de los usuarios; cuando se habla de seguridad informática debemos hacer referencia al virus informático y el software utilizado por el lenguaje de programación compuesto por

ordenadores intangibles. El virus tiene como objetivo dañar o infectar los sistemas informáticos y se externaliza al robo de información.

De modo similar, Romero (2018) señala que los pilares que conforman el sistema digital son la confidencialidad, integridad y disponibilidades. Estos son concebidos como fundamentos esenciales de la seguridad digital. Es importante incorporar mecanismos preventivos que consisten en la incorporación de mejoras en el hardware y software para evitar así el impacto de los ciberataques y ser víctimas que programaciones maliciosas como troyanos, gusanos, blackdoors que atenten con los ordenadores tecnológicos

i. Definición del Phishing

El *phishing* se define como una de las técnicas usadas por los delincuentes. Es un tipo de fraude que usa el engaño para manipular a las víctimas; el *phishing* se traduce como pesca fishing, definiéndose como un tipo de pesca para que los usuarios del internet incurran en error. Es una de las técnicas de ingeniería social más conocidas en el mundo virtual. Este puede efectuarse mediante 2 modalidades básicas: la primera suplantar la identidad del personal bancario para obtener información confidencial y la segunda se genera usando comunicaciones electrónicas, como correos y llamadas tecnológicas.

En la misma línea, el Observatorio Peruano de Cibercriminalidad-Fraudes Virtuales (2020), define al phishing como una modalidad que busca a personas más vulnerables en la red. Mediante técnicas de ingeniería social, los atacantes simulan ser entidades bancarias o empresas para incurrir en error al usuario. También esta modalidad se realiza mediante el envío de correos electrónicos que dirigen a una página falsa para obtener el código y contraseña, permitiéndole obtener información personal.

ii. Definición del Smishing

Esta terminología es usada por los ciberdelincuentes para cometer fraudes informáticos, el smishing es una de las formas del phishing mediante el cual el agente activo intenta obtener información privada a través de mensajes de texto. El termino smishing está compuesto por la contracción de las siglas en ingles SMS que en español significa “mensaje corto de texto”.

La modalidad se emplea mediante mensajes fraudulentos que dirige al agente pasivo, para que este vaya a un sitio web, o una llamada telefónica derivándolos a un número. Los ciberdelincuentes tienen un perfil específico para cometer el acto fraudulento

validándose de las necesidades básicas o la obtención de un premio ficticio con el fin de develar datos personales.

En relación a esto, García (2021), explica que la exposición a un nuevo mundo virtual implica que cada vez es más frecuente el uso de teléfonos inteligentes, y con ellos ataques del smishing. Tanto como el *smishing* y *el phishing* son modalidades muy parecidas, mientras que el phishing se realiza mediante correos electrónicos, el smishing se efectúa mediante mensajes de texto con la finalidad que los usuarios faciliten información valiosa. El smishing ha resultado una de las modalidades más preocupantes de la seguridad informática ya que es más fácil el bloqueo del phishing con ordenadores que el smishing debido a que resulta más fácil tener acceso directo a una página con un enlace.

iii. Definición del Vishing

Esta modalidad de estafa pretende suplantar la identidad afectando a través del VOIP “voz sobre protocolo de Internet IP” recreando una voz automatizada, semejante al de las entidades bancarias. La terminológica del *vishing* proviene de la unión de voice -phishing. Dicha modalidad se produce mediante llamadas tecnológicas suficiente para llamar la atención del usuario para que proporcione información confidencial.

A favor de tic (2017), cuando sostiene que “consiste en obtener datos de otra persona para utilizarlos como si fueran propios. Generalmente con el objetivo de realizar trámites legales, bancarios o de seguros y compras”

En esta modalidad de estafa informática el agente activo utiliza los medios tecnológicos como teléfono y correo electrónico. La finalidad es robar la identidad y el dinero de los usuarios. El *vishing* es una de las modalidades más comunes usadas por los cibercriminales; mediante el envío de correos electrónicos que solicitan que llamen a un número de teléfono donde aparece un contestador automático.

Desde el mismo modo, López (2021), nos habla que es una técnica que se emplea mediante llamadas telefónicas usando contestadoras automáticas, robóticas o dejando correos de voz suplantando así la identidad de un supuesto familiar para concretar el acto ilícito.

El bien jurídico protegido por la criminalidad informática

Para definir el bien jurídico tutelado de los delitos informáticos primero debemos analizar la existencia de la vulneración del interés jurídico. Debemos tener en consideración que el bien jurídico es aquel derecho intangible que la ley busca proteger. En ese sentido, es menester considerar la necesidad de protección jurídica penal.

El uso de sistemas informáticos tiene relación con el desarrollo social y económico de cada país. Esta realidad ha generado la aparición de nuevas modalidades de comisión delictivas; por ende, bienes jurídicos que ameritan de una protección legal. Esta modalidad delictiva viene causando perjuicios en sus distintas magnitudes. Cabe destacar que el legislador tiene que recoger estas nuevas modalidades delictivas para prevenir y sancionar los delitos de carácter informático, y partir de ello para materializar la protección de determinados bienes jurídicos, seguridad informática y patrimonios pluriofensivos.

Al respecto, Coello (2020) sostiene que la criminalidad informática no solo protege bienes jurídicos patrimoniales, sino también bienes jurídicos supraindividuales vinculados a la intangibilidad del tráfico de información en la red. Así mismo sostiene que el bien jurídico a protegerse reviste de contenido patrimonial y/o extrapatrimonial. En este sentido, ya no nos estaríamos enfrentando solamente a intereses patrimoniales o extrapatrimoniales sino también a la seguridad de comunicaciones informática.

Los delitos informáticos contenidos en la ley n.º 30096, Ley de delitos informáticos, están orientados a proteger bienes jurídicos de carácter patrimonial, dejando de lado otros intereses como viene siendo la seguridad informática, y con ello no se estaría cumpliendo con las finalidades de bienes jurídicos para proteger su integridad.

1.1.4. Definición de términos básicos

Es importante definir hasta este punto palabras técnicas y complejas utilizadas para la investigación y algunas propias del dialecto informático. Estos términos se desarrollan con el propósito de tener mayor comprensión acerca de la investigación realizada.

- **Tratado Internacional:** Según la Organización de los Estados Americanos (1969), menciona que es “un acuerdo internacional celebrado por escrito entre Estados y regido por el derecho internacional, que conste en un instrumento único o en dos o más instrumentos conexos”.

- **Delitos informáticos:** Conforme al diccionario Panhispánico del español Jurídico (2020) “es la Infracción penal cometida utilizando un medio o un instrumento informático”.
- **Ciberdelito:** La presente definición es a favor del TIC (2017): “es un crimen que se comete a través de las plataformas digitales donde el agente puede ser cualquier persona.
- **Cibercrimen:** El cibercrimen es una actividad delictiva que afecta o abusa de una computadora o una red informática.
- **Ciberespacio:** En palabras de Álvarez (2018), quién sostiene que “cabe entender ese espacio no físico donde se interconectan e interrelacionan las redes de comunicación donde las personas pueden interactuar e intercambiar información”.
- **Ciberdelincuencia:** Puede entenderse en sentido estricto, comprendiendo cualquier comportamiento ilícito realizado mediante operaciones electrónicas que atentan contra la seguridad de sistemas informáticos y datos que se procesan (2018).
- **Ingeniería Social:** Es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica usada por los ciberdelincuentes para obtener información, acceso o permisos en sistemas de información que les permitan realizar daños al usuario o persona jurídica (2020).

1.2. Formulación del problema

1.2.1 Problema General

¿Las modalidades delictivas del *Phishing*, *Smishing* y *Vishing* se encuentran recogidas en la legislación peruana?

1.2.2 Problema Especifico

¿Cuáles son los elementos que deben ser considerados a fin de tipificar las conductas delictivas del *phishing*, *smishing* y *vishing*?

¿Qué naturaleza jurídica debe adoptar la tipificación de las conductas delictivas del *phishing*, *smishing* y *vishing*?

1.3. Objetivos

1.3.1 Objetivo General

Justificar por qué los delitos del *phishing*, *smishing* y *vishing* deben ser incorporados en el Sistema Penal como delitos penalizados en el Perú.

1.3.2 Objetivo Especifico

- Identificar cuáles son los elementos que deben ser considerados a fin de tipificar las conductas delictivas del *phishing*, *smishing* y *vishing*.
- Determinar la naturaleza jurídica que debe adoptar la tipificación de las conductas delictivas del *phishing*, *smishing* y *vishing*,

1.4. Hipótesis

1.4.1 Hipótesis General

Las modalidades delictivas del *phishing*, *smishing* y *vishing* no se encuentran reguladas en la legislación peruana, en ese sentido, a la fecha existe cierta impunidad de estas conductas.

1.4.2 Hipótesis Especifico

- Los elementos relevantes de carácter penal que deben ser tomadas en cuenta para las estructuraciones de los tipos penales del *phishing* son utilización de correos electrónicos en la que se incorpora medios digitales fraudulentos con fines de obtener información de terceros; por su parte el *Smishing*, consideramos que tener contener la utilización de mensajes de texto en que la se incorpora medios digitales con fines defraudatorios; y con respecto al *vishing*, se debe considera los actos referidos a la utilización de llamadas telefónicas robotizadas y/o personales con fines defraudatorios.

- Los delitos que contemplen las conductas delictivas del *phishing*, *smishing* y *vishing* deben ser de naturaleza de delitos de mera actividad o delitos de peligro.

Justificación de la Investigación

La presente investigación se justifica con la necesidad tipificar los delitos *phishing*, *smishing* y *vishing* en el sistema penal peruano y la Ley n.º 30096 de delitos informáticos y su modificatorio n.º 30171, donde se regula intrínsecamente aquellos actos ilícitos que se realizan en el sistema Informático vulnerando así derechos fundamentales mediante dichos actos cometidos a través el uso inadecuado de la tecnología, atentando contra la información y privacidad. El objeto de la investigación es analizar la importancia de la incorporación del *Phishing*, *Smishing* y *Vishing* para combatir la lucha contra la ciberdelincuencia en el Perú y los riesgos que generarían para la sociedad, empresas si no se encuentran tipificadas.

Dicha necesidad nace de la realidad que subyace en el país; ya que nos encontramos frente a una era tecnológica ascendente. Una herramienta que ha facilitado la vida de muchas personas; sin embargo, cuando la tecnología es empleada de forma maliciosa, puede transgredir bienes jurídicos y de este modo sacar provecho económico. Esta se ve reflejada por el gran número de denuncias informáticas que presenta la DIVINDAT. Por otra parte, si bien es cierto que tenemos leyes como la ley n.º 30096 y su modificatorio n.º 30171 sobre la protección de delitos informáticos, estas no serían suficientes para evitar el crecimiento de los delitos informáticos, lo que imposibilita el desarrollo de determinados actos en vía penal al no poder encontrarse reguladas en la norma. Es por ello que al no ser reguladas generan una sensación de impunidad para la sociedad, ya que no se podrían proteger correctamente sus derechos causando un perjuicio grave a las víctimas.

Por consiguiente, este trabajo de investigación busca penalizar los delitos del *Phishing*, *Smishing* y *Vishing* con la finalidad de proporcionar seguridad jurídica a todos los usuarios que utilizan constantemente medios tecnológicos. Como resultado de dicha regulación se beneficiaría a todos los ciudadanos para no ser presas fáciles de los delitos informáticos y proporcionar sosiego a la sociedad.

CAPÍTULO II. MÉTODO

2.1 Tipo de Investigación

En esta perspectiva de la investigación es imprescindible establecer los criterios para la metodología empleada. Para empezar, el nivel investigativo es el exploratorio. Según Arias (2021), esto hace referencia a descubrir información con un objetivo de estudio desconocido; buscando la aproximación a fenómenos novedosos. Una de sus principales características es que este tipo de investigación carece de información y la utilización de la observación y métodos cualitativos.

No obstante, el nivel de aplicación de la investigación es el básico o puro, mediante el cual Navarro (2016) señala que la finalidad es adoptar nuevas teorías o modificar ya las establecidas, de modo que se logre incrementar los conocimientos científicos. Asimismo, busca la recolección de datos y descubrir principios o leyes para dar pie a soluciones en el ámbito social. Por el contrario, estas investigaciones no tienen el objetivo de utilizarlas de modo inmediato, pero tampoco esta desligado a la práctica de la investigación.

El enfoque para la investigación es el cualitativa, ya que como parte del marco teórico tiene como finalidad explicar la importancia de incorporar los delitos del *Phishing*, *Smishing* y *Vishing*. Tal como lo señala Maldonado (2018), la investigación cualitativa posee un enfoque multi metódico donde el sujeto de estudio es interpretativo y naturista mediante el cual el investigador estudia la interpretación de los fenómenos naturales con un valor que pretende analizar, traducir y describir para la investigación de fenómenos sociales.

Para la realización de la entrevista se empleó un enfoque mixto concurriendo en el enfoque cualitativo. Vargas (2013), nos señala que es una técnica para recoger datos y un conjunto de instrumentos altamente estructurado, es decir el abordaje tiene una perspectiva cualitativa y está orientado para que el entrevistado hable de forma directa.

2.2 Población y muestra (Materiales/Instrumentos)

2.2.1 Población

El estudio de la investigación planteada se basa en lo definido por Medina (2018) en su artículo titulado “Técnicas e instrumentos de la Investigación”, donde propone que:

La tipología de la información cualitativa-cuantitativa deben estar justificadas por los objetivos, hipótesis de la investigación, las técnicas son empleadas para recolectar información es por ello la necesidad de realizar encuestas, cuestionarios y entrevistas (p.10).

En efecto, se tiene la necesidad de una selección adecuada del objeto de estudio y el planteamiento de la problemática de la investigación con la finalidad de obtener recursos para el buen desarrollo de la investigación. Asimismo, Mejía (2005) explica que la población es el conjunto de sujetos con un objeto común, que concuerdan con determinadas especificaciones. También se constituye del número de participantes, de modo que el investigador plantea la hipótesis con el objetivo de analizar mediante la población y muestra el tipo de investigación.

Como resultado, habiendo aclarado algunas definiciones de la investigación, se estableció como población finita a un grupo de abogados y fiscales especializados en el tema, tomando como base la información proporcionada por el Ministerio Público y Poder Judicial vía online, Convenios internacionales, leyes sobre delitos informáticos, los cuales fueron analizados cuidadosamente. De esta forma se buscó responder la importancia de incorporar las modalidades del *Phishing*, *Smishing* y *Vishing* en nuestro sistema penal.

2.2.2 Muestra

Posteriormente López (2004), señala que la muestra es el espacio abstracto que es materia de estudio y que hace una representación a la población para entonces así sacar conclusiones. Es un tipo de herramienta de la investigación científica para analizar a todos los elementos de una población y hacer inferencia sobre la población. Para que el muestreo sea eficiente, debe componerse de las similitudes y diferencias encontradas en la población.

Asimismo, la muestra de la investigación es la recopilación de datos que proporciona la población materia de la investigación para así señalar elementos que nos lleven a esclarecer las hipótesis de nuestra investigación tal como lo señala Tomayo (2002), quien menciona en su obra “El proceso de la Investigación Científica”:

Una de las características de la muestra es establecer los objetivos de estudio consiste en encontrar elementos de la investigación en base a los resultados de los integrantes de la población el cual posibilita la predicción probabilística de la población.

En tal sentido, la muestra estuvo conformada por 3 abogados especialistas en ciberdelincuencia, entre ellos 2 fiscales, 1 miembro de la Policía Nacional del Perú (DIVINDAT); todos ellos con una amplia trayectoria académica profesional. Se consideró también información obtenida sobre delitos informáticos, reporte sobre Ciberseguridad 2020 realizada por la OEA, materiales complementarios obtenidos por el Ministerio Público y Poder Judicial.

2.3 Operacionalización de variables

OG: Justificar por qué los delitos del *phishing*, *smishing* y *vishing* deben ser incorporados en el Sistema Penal, como delitos penalizados en el Perú.

Tabla 1

Operacionalización de las variables dependiente e independiente

Variables	Definición conceptual	Dimensión	Indicadores
V_D: Sistema Penal del Perú 2020.	<p>El convenio de Budapest (Tratado Internacional Europeo)</p> <p>Convenio Internacional sobre Ciberseguridad un tratado adoptado por el Consejo Europeo el 2001, y adherido en el Perú el 2019 con la finalidad de afrontar nuevas amenazas de la era digital cuyas características es la creación de un marco de derecho penal sustantivo.</p> <p>La Ley N°30096 (Delitos Informáticos):</p> <p>El tratamiento de los Delitos Informáticos estaba regulado en el Código Penal de 1991, pero dicha tipificación no era suficiente, no obstante gracias a la promulgación de la Ley N°30096 y su modificatoria de la Ley N°30171, ley de Delitos Informáticos con la finalidad de poder hacer frente a la criminalidad digital.</p>	Ley N°30096	Ciberdelincuencia
			Delitos informáticos
V_I: Incorporar delitos como el phishing, smishing y vishing.	<p>Estas modalidades son consideradas como un tipo de fraude para robar información confidencial.</p> <p>Phishing: (el fraude se efectúa por envíos de correos electrónicos)</p>	Administración de Justicia	Proceso Judicial
			Ministerio Público
			Poder Judicial
			División de Investigación de Delitos de Alta Tecnología

	<p>Smishing: (el fraude es cometido mediante mensajes de texto)</p> <p>Vishing:(suplantar la identidad a través de voces automatizadas)</p>		
--	---	--	--

Fuente: Elaboración propia

2.4 Técnicas e instrumentos de recolección y análisis de datos

Para lograr recolectar estructuralmente la información recogida se emplearon una serie de procedimientos según lo señalado por Arias (2020). Una de las formas de obtener información y recolectar datos fundamentales para la investigación es un medio para almacenar datos recogidos de las variables, según lo reafirmado por Artega (2020) como una de las técnicas para la aplicación sistemáticas de los datos. Dicho procedimiento se puede representar en tablas y gráficos, de tal modo que se obtengan conclusiones esenciales para la obtención de datos para la investigación eliminando conclusiones innecesarias.

En tal sentido, Persman (2014) manifiesta que la aplicación adecuada para la recolección de datos debe orientarse a una serie de combinaciones de pruebas empíricas necesarias para recolectar información contenidos en libros o documentos cuya utilidad es servir como fuentes verídicas (p.10).

En concordancia con lo expuesto con anterioridad debemos precisar técnicas e instrumentos practicados. Por otro lado, se procedió con la aplicación del instrumento de recolección de datos del análisis de documento. La estrategia elaborada para la búsqueda fue obtener información proporcionada por el Ministerio Público, informes sobre ciberseguridad, análisis de leyes y convenios, con la finalidad de describir documentos de forma sistemática incluyendo bibliografías. Posteriormente se realizó el muestreo y se aplicó el descarte por orden ascendente desde 2014-2020 hasta la actualidad.

Los documentos analizados registran información relevante para el tema de estudio. También se consideró el informe de análisis N.º 4, una estrategia contra la criminalidad 2021 de la cantidad de casos resueltos por las fiscalías provinciales por denuncias relacionados por delitos informáticos sobre la Ley n.º 30096.

Posteriormente, para delimitar la información, se muestran ordenadores visuales y se incorpora figuras con la finalidad de explicar el objetivo general y los objetivos específicos de la investigación realizada. Cabe mencionar que para el desarrollo del trabajo se tomó en cuenta información obtenida vía web. De acuerdo a la obtención y el análisis virtual de la información se creyó pertinente la incorporación de la siguiente tabla.

Tabla 2

Análisis virtual de documentos

Análisis de documentos

Criterios	Análisis virtual
Materiales	1 laptop con acceso a internet, libros, revistas, periódicos.
Sistematización	Sistema de Información de Apoyo al Trabajo Fiscal
Costo	Costo de internet y energía eléctrica.
Resultados de la investigación	Información proveniente de páginas oficiales del Ministerio Público, por lo que resulta confiable.

Fuente: Elaboración propia

Por otro lado, se aplicó entrevistas para mejorar la comunicación interpersonal con el fin de obtener respuestas verbales a las interrogantes presentadas por el tema de investigación. Por ello, se optó por realizar entrevistas a 3 abogados y 2 fiscales especializados en la materia, así como a 1 miembro de la DIVINDAT.

El instrumento de recolección de datos fue el cuestionario o guía de entrevistas. Se realizó 2 entrevistas, las primeras 5 preguntas corresponden al objetivo general, 5 preguntas vinculadas al objetivo específico, haciendo un total de 10 preguntas. Asimismo, se realizó una segunda entrevista conformada por 5 preguntas para hacer un análisis acerca de los casos atendidos por la División de Investigaciones de Delitos de Alta Tecnología.

Tabla 3

Entrevista virtual

Entrevistas

Criterios	Aplicación virtual
Población	Abogados especialistas en ciberdelincuencia en el ámbito nacional, fiscales y un miembro de la DIVINDAT.
Materiales	Una laptop con acceso a internet.
Tiempo	Entre 30 a minutos.
Costo	Internet, plataforma Zoom y energía eléctrica.
Lugar	En el país de Perú y departamento de Lima mediante la Plataforma digital de Zoom Meetings.
Entorno	Entrevista personalizada sin participación de sujetos externos.
Rasgos conductuales	Profesionalismo, conocimiento y dominio del tema.
Resultados de la investigación	Información pertinente y confiable.

Fuente: Elaboración propia

Recapitulando, ya habiéndose establecido de forma clara el método utilizado para el proceso de la investigación es importante detallar el procedimiento de la investigación y hacer precisión sobre los modelos utilizados para la entrevista.

2.5 Procedimiento

2.5.1 Procedimiento de recolección de datos

Para empezar, procederemos a la explicación de la recolección de datos. Se consideraron una serie de criterios para la obtención de información requerida para la investigación. Uno de los más relevantes es que se precisó el aspecto temporal desde el 2014 hasta el 2020. No obstante, se delimitaron el estado de la investigación, el delito investigado, los códigos usados, la etapa preliminar, el tipo de conclusión. Asimismo, se analizó el aspecto espacial, que sería en todo el país, ya que su regulación beneficiaría a todos los ciudadanos, considerando para ello el distrito fiscal en el que se siguió la investigación.

En un segundo momento, se aplicó el instrumento de recolección de datos de la entrevista, siendo una herramienta importante para recolectar los testimonios de agentes especializados sobre la ciberdelincuencia. Posteriormente, se realizó un listado de todos los participantes de la entrevista con su respectivo cargo e instrucción.

Al terminar de redactar los objetivos de la presente investigación se formularon las preguntas siguiendo el criterio de aplicación por espacio geográfico. Dicho de otro modo, 10 preguntas formuladas para los fiscales y abogados y 5 preguntas para la División de Investigaciones de Delitos de Alta Tecnología, ya que todas se desprenden del objetivo general y de los objetivos específicos.

2.5.2 Procedimiento de tratamiento de análisis de datos

- El procedimiento de análisis de los documentos se realizó información proporcionada por el Ministerio Público y el Poder Judicial, además se hizo una subdivisión para colocar en una de ellas la información general.
- Los pasos realizados fueron en primer término la conversión del archivo PDF en formato Excel para colocar, ordenar y filtrar las celdas pertinentes. Esto permitió que se pueda ordenar la información en gráficos dinámicos y que se evidencie los resultados de forma transparente y sencilla.
- La plataforma Zoom fue la herramienta digital elegida para efectuar las entrevistas porque facilita al entrevistador generar un link de invitación prefijando la fecha y

la hora el cual se producirá la entrevista. Todo esto se realizó de manera respetuosa, ya que muchos de los entrevistados preferían que no se le tomara fotos.

2.6 Aspectos éticos

Cabe señalar que durante el desarrollo de la investigación se respetó criterios éticos, entre ellos, conforman la redacción académica en cuanto al citado y las referencias bibliográficas, además que los reportes fueron obtenidos a través del conducto regular, el acceso a la información público. Además, debe explicarse que para la realización de la entrevista se pidió que otorguen su consentimiento verbal para ser grabados para el desarrollo de la investigación. No obstante, se tuvo en consideración que muchos de los entrevistados prefirieron que no se le tomaran fotos.

Con respecto a la credibilidad se respetó todos los hechos y hallazgos producidos dentro de la investigación, los resultados reflejan la realidad de la problemática social.

Adicionalmente, dentro de la investigación se ha respetado las fuentes de información, las mismas que se han citado correctamente según el formato APA proporcionado por la Universidad Privada del Norte. También se ha respetado los lineamientos que la universidad consigna para hacer viable la aprobación de una tesis, ya que la investigación debe estar orientada a un beneficio social. Cabe destacar que la información obtenida provino de fuentes fidedignas, mostrando así la transparencia de la investigación.

CAPÍTULO III. RESULTADOS

En este trabajo se propuso realizar el análisis e interpretación de los hallazgos obtenidos mediante una minuciosa búsqueda, que incluyó los resultados de los análisis documentales empelados en la investigación del Ministerio Público, además del análisis de las entrevistas a los 5 especialistas nacionales y 1 efectivo policial de la División de Investigación de Delitos de Alta Tecnología. A continuación, se mostrará los resultados del análisis de la legislación.

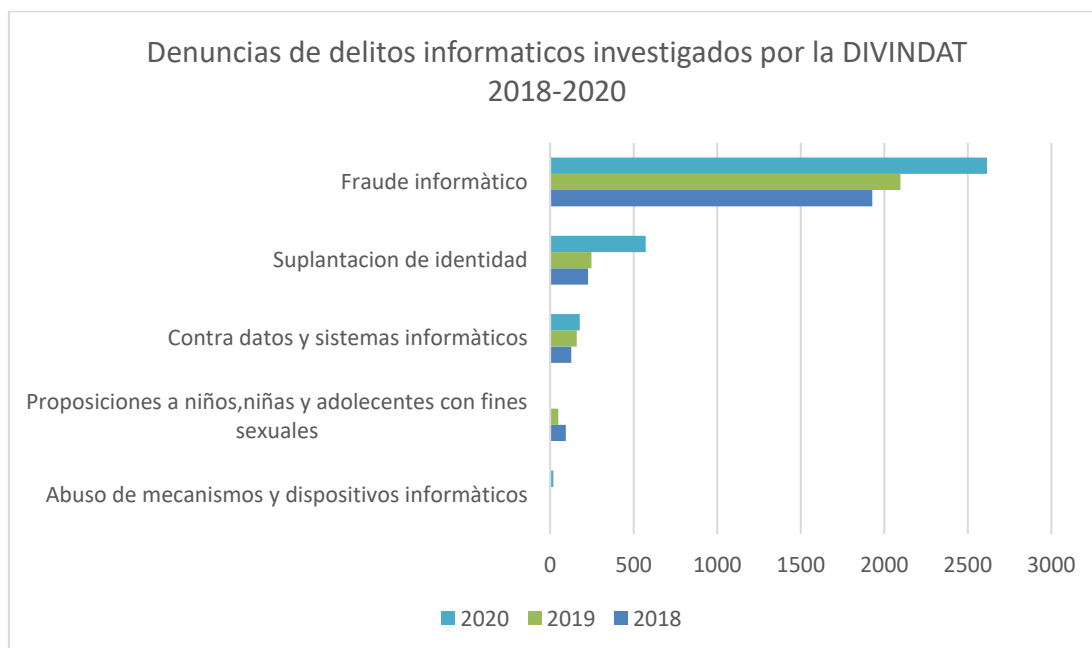
3.1 Resultados de análisis documental

3.1.1 Análisis documental del Ministerio Público

Para comenzar estos reportes son proporcionados por el Ministerio Público sobre las denuncias registradas por la División de Delitos de alta Tecnología en un margen temporal entre octubre 2018 a diciembre de 2020. A partir de estos, se procedió a elaborar organizadores visuales en forma de figuras con el propósito de tener un mejor entendimiento y con ello evaluar el registro de casos vinculados a la Ley n.º 30096 y el incremento anual de casos relacionados a delitos informáticos y el tratamiento que le da el Sistema penal.

Figura 1

Análisis de denuncias de delitos informáticos investigados por la DIVINDAT. 2018-2020

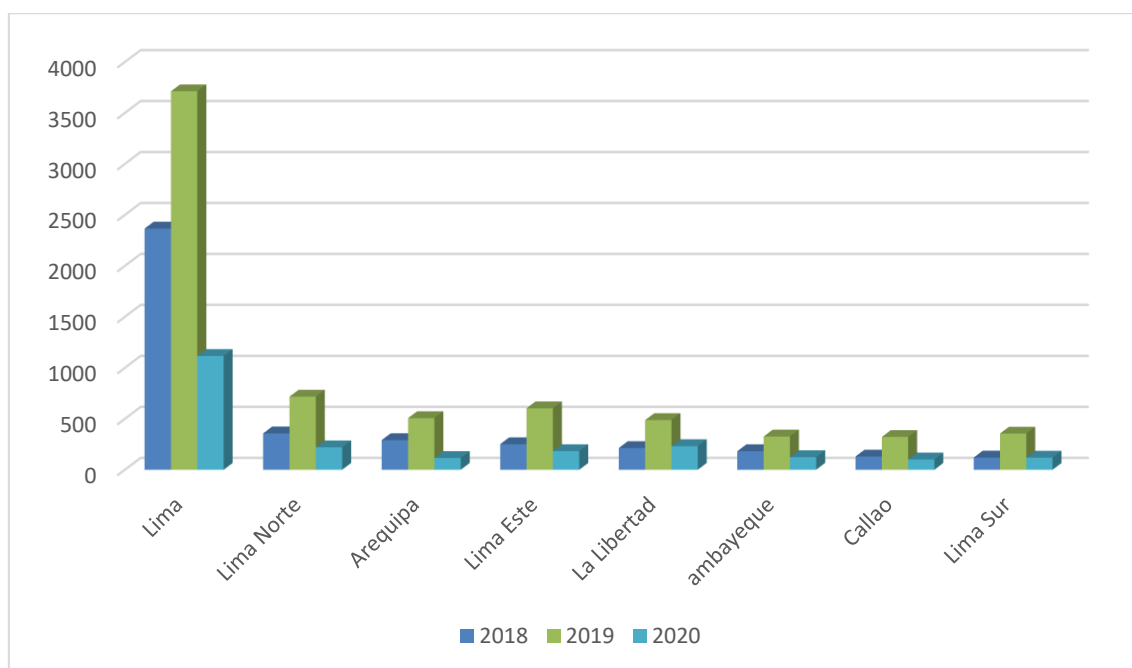


Fuente: Elaboración propia a partir del Informe N°4 del Ministerio Público y la oficina de análisis de estratégico contra la criminalidad.

Interpretación: La figura muestra las denuncias realizadas por delitos informáticos desde el periodo del 2018 hasta el 2020. Se puede observar un aumento progresivo durante estos tres últimos años teniendo en cuenta que contamos con la adhesión al convenio de Budapest desde el 2019 mediante la Ley n°. 30096 y su modificatoria. Esto nos hace señalar que la mayoría de los casos tienen mayor incidencia en el delito de fraude informático con un porcentaje de 78.2% y consecuentemente el delito de suplantación de identidad 12.6%. Por otro lado, se podría señalar que aún no son suficientes los mecanismos que emplean nuestro sistema jurídico para el tratamiento de estas modalidades, así como la importancia de incorporar nuevos ilícitos penales para contrarrestar la ciberdelincuencia.

Figura 2

Análisis por denuncias por delitos informáticos registradas en Fiscalías Penales Comunes y Fiscalías Mixtas, de octubre 2018 a julio 2020.



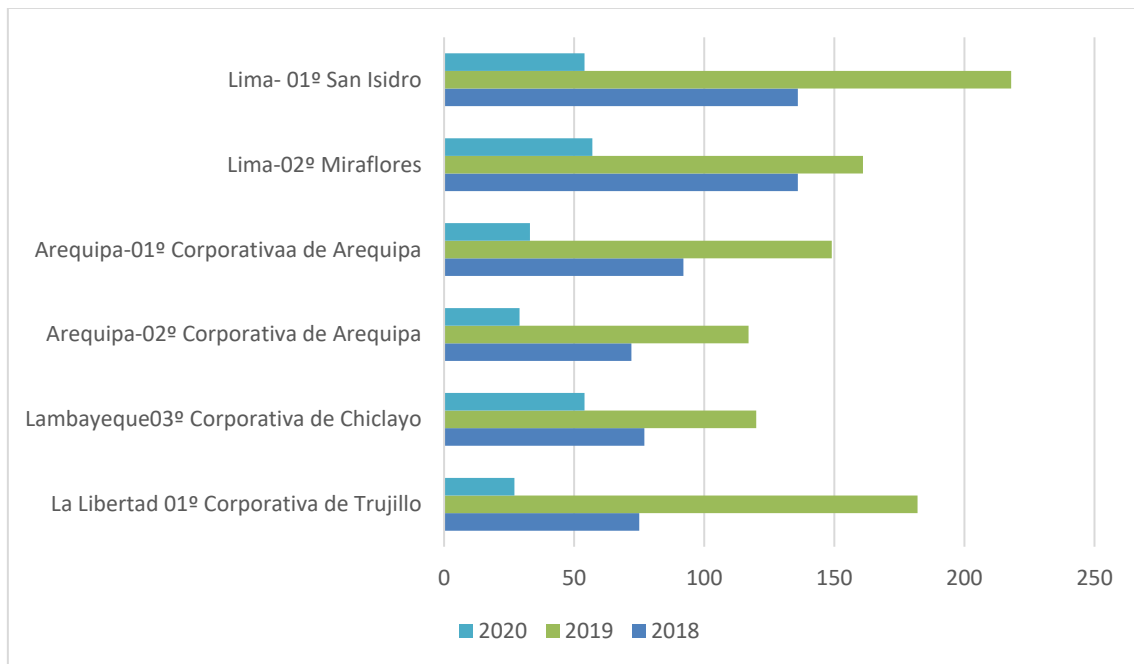
Fuente: Elaboración propia a partir de la Oficina de Racionalización y Estadística del Ministerio Público.

Interpretación: En esta figura podemos analizar las denuncias realizadas por delitos informáticos Ley n°. 30096, entre Fiscalías Penales Comunes Especializadas y Fiscalías Mixtas que suman un total de 21,687 denuncias; y las del Distrito Fiscal de Lima, con un total de 7668 denuncias recibidas incluidas Lima Norte, Arequipa, Lima Este, La Libertad, Lambayeque, Callao y Lima Sur. De este modo, podemos inferir que las denuncias muestran un incremento anual, dándonos a entender que a pesar de los

esfuerzos de las fiscalías y los ordenadores jurídicos no pueden imputar la responsabilidad correctamente debido a la falta de tipificación del acto ilícito en las modalidades que comúnmente los ciberdelincuentes usan para defraudar a las personas como el *phishing*, *smishing* y *vishing*.

Figura 3

Análisis de casos de las Fiscalías con mayor cantidad de registros por delitos informáticos desde el periodo del 2018 al 2020.

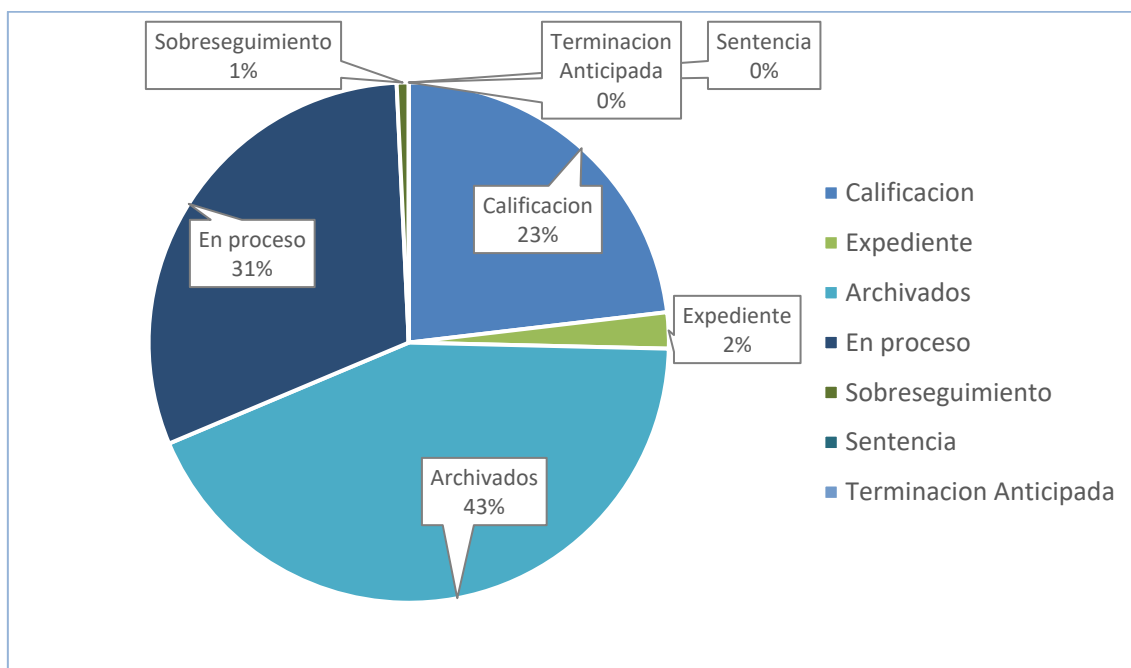


Fuente: Elaboración propia a partir del reporte de la Oficina de Racionalización y Estadística.

Interpretación: Como podemos observar en la figura, la fiscalía con mayor cantidad de registros por delitos informáticos entre el año 2018, 2019 y 2020 es en el distrito fiscal de Lima, entre San Isidro y Miraflores con un total de 762 denuncias durante los periodos mencionados; en segundo lugar, el distrito fiscal de Arequipa con un total de 572 denuncias, Lambayeque con un total de 251 denuncias, y La Libertad con un total de 284 denuncias recibidas.

Figura 4

Análisis del estado procesal de denuncias por delitos informáticos 2013 al 2020.

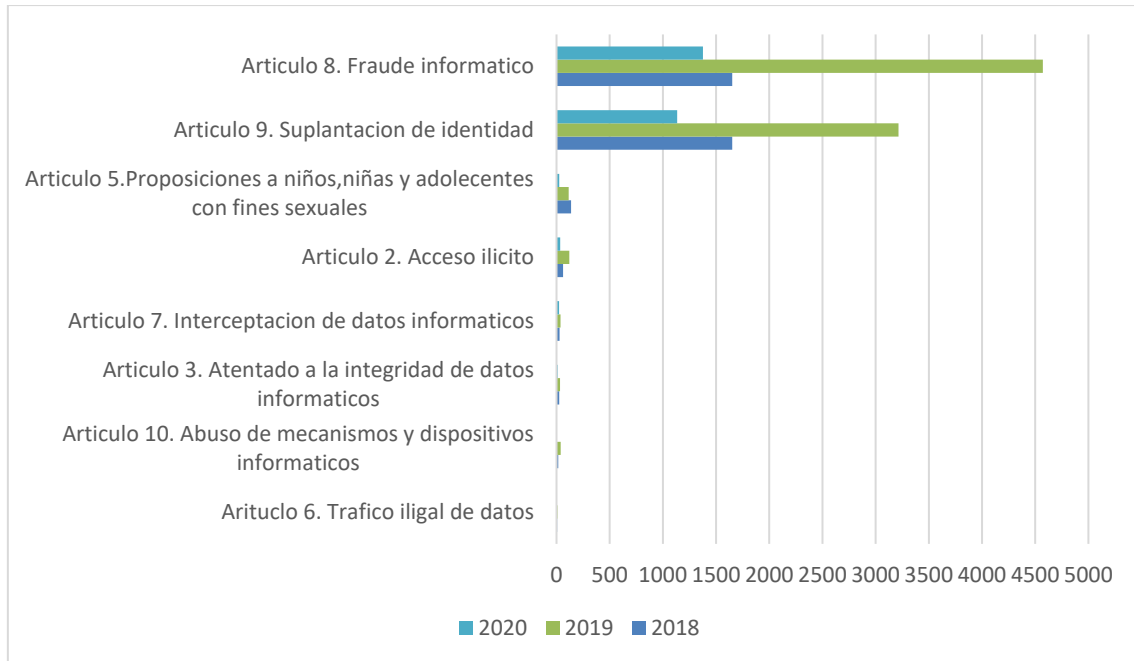


Fuente: Elaboración propia a partir Oficina de Racionalización y Estadística, remitido a la OFAEC.

Interpretación: La figura muestra dentro de la calificación, expediente, archivados, en proceso, sobre seguimiento, sentencia y terminación anticipada, sumando un total de 23,657 denuncias. De estas, un 58% (12608) han sido archivadas y un 41% (8842) que se encuentran en proceso de investigación. En tal sentido, muchos de los casos de delitos informáticos no llegan a la imputación de la pena debido a que existe algunas deficiencias en el proceso de la investigación, como la conversación de la prueba digital y la proposición de actos de investigación. De este modo terminan archivándose en investigación preparatoria. Se debe considerar que ni el Ministerio Publico ni el Poder Judicial cuentan con una adecuada infraestructura ni material logístico idóneo, creando impunidad legal a la sociedad por la falta de tipificación de la norma. Es por ello que la investigación busca encajar el delito del *phishing*, *smishing* y *vishing* en el Sistema Penal.

Figura 5

Análisis de denuncias de delitos informáticos según la Ley n.º 30096.

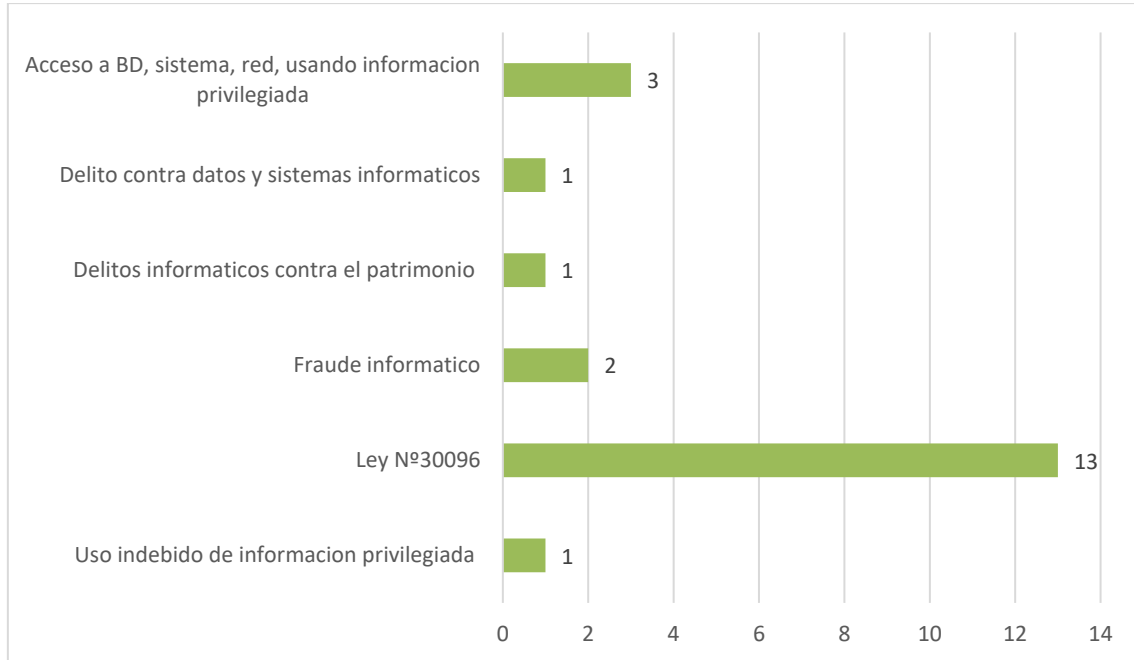


Fuente: Elaboración propia a partir del reporte de la Oficina de Racionalización y Estadística, remitido a la OFAEC.

Interpretación: Los datos mostrados en la figura muestran el incremento anual de Fraudes informáticos, que suman el 37.8% del total de (6001). A continuación, el delito Suplantación de identidad, que representa el 3.8% con un (611) de casos imputados para este delito, luego el delito de Propositiones a niños, niñas y adolescentes con 1.7% (277) de denuncias, el delito de Acceso ilícito 1.4% (216) de denuncias, Interceptación de datos informáticos 1.4% (216), delitos Atentado a la integridad de datos informáticos 0.4% (68), delito de Abuso de mecanismos y dispositivos informático 0.4% (58) de denuncias, delito de Tráfico ilegal de datos 0.1% (20). A partir de estas cifras podemos inferir el incremento de delitos informáticos, que, a pesar de contar con instrumentos jurídicos para contrarrestar los delitos informáticos, no son suficientes para combatir la cibercriminalidad.

Figura 6

Análisis de Delitos informáticos registrados en las Fiscalías Especializadas contra la Criminalidad Organizada.

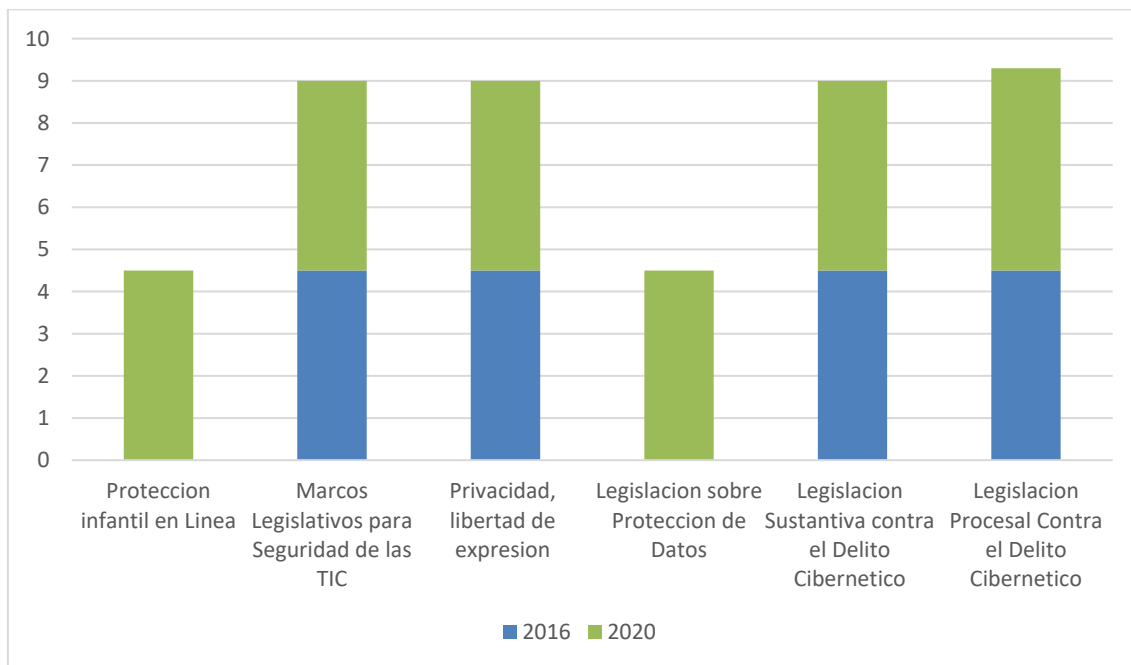


Fuente: Elaboración propia a partir de los datos obtenidos por la información proporcionada por la Fiscalía Superior Nacional Coordinadora de Fiscalías Especializadas contra la Criminalidad Organizada.

Interpretación: La figura muestra que los delitos con mayor incidencia son los delitos informáticos de la Ley n°. 30096 cuyo registro son específicamente por las Fiscalías Especializadas contra la Criminalidad Organizada en el periodo de noviembre 2020. Esto hace referencia a que existe una necesidad legal de incorporar los delitos del *phishing*, *smishing* y *vishing* como ilícitos supraindividual protegiendo así la seguridad informática.

Figura 7

Análisis de marcos legales y regulatorios desde el periodo 2016 al 2020.



Fuente: Elaboración propia a partir del Reporte sobre Ciberseguridad 2020 proporcionado por la ONU y OEA.

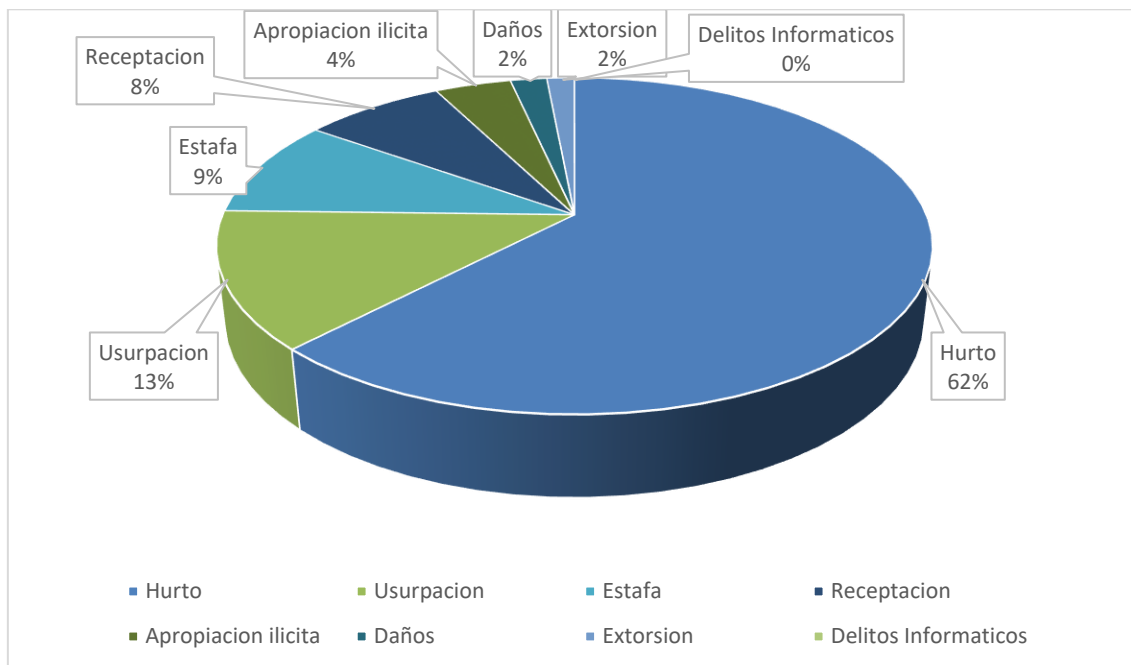
Interpretación: Como podemos apreciar, el Perú ha tenido un gran crecimiento durante el periodo del 2020 en cuanto a la regulación de marcos legislativos para combatir la ciberdelincuencia, sobre todo en protección infantil en línea y legislación sobre protección de datos. Podemos enfatizar que existe un avance normativo durante el periodo del 2016 al 2020, no obstante, podemos apreciar en cuanto a la regulación de marcos legislativos para seguridad de las TIC, privacidad libertad de expresión, legislación sustantiva contra del delito cibernético y legislación procesal contra el delito cibernético estos no han logrado un avance normativo en cuanto el periodo del 2016 al 2020. De este modo podemos inferir que, teniendo en cuenta la realidad virtual, esto no es suficiente para estar a la vanguardia de las necesidades tecnológicas de una sociedad.

3.2 Análisis documental del Poder Judicial

A continuación, se mostrará los análisis documentales proporcionados por el Poder Judicial, con el fin de responder a nuestras variables e hipótesis planteadas. Para mejorar la presentación de la información se realizó figuras para dar mejor entendimiento, cada uno de ellas con una interpretación a partir de los datos mostrados.

Figura 8

Análisis de personas con sentencia condenatoria por delitos contra el patrimonio 2017.

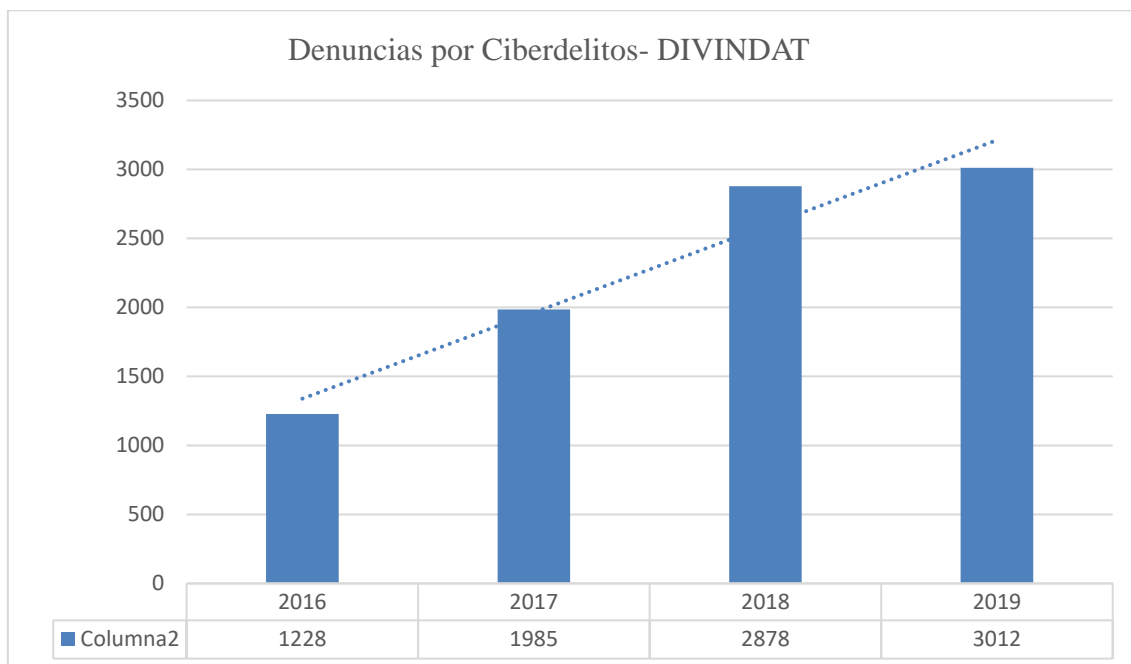


Fuente: Elaboración propia a partir de Poder Judicial - Registro Nacional de Condenas.

Interpretación: La figura nos muestra que la modalidad con más incidencia es la de delitos de patrimonio, en su mayoría delitos de hurto y robo con un total de 16,870 casos con sentencia condenatoria. No obstante, cabe mencionar que en el periodo del 2017 solo existe 2 casos con sentencia condenatorio por delitos informáticos; es decir, muchos de los casos por delitos informáticos ni siquiera llegan a sentencia con un 58% de procesos que se archivaron ya sea por la dificultad para identificar el autor o la necesidad de equipos de alta tecnología para combatir la ciberdelincuencia, falta de peritos y la necesidad de pericias de dispositivos electrónicos o equipos informáticos para determinar el IP del agente activo.

Figura 9

Análisis de número de denuncias recibidas por la DIVINDAT entre el periodo del 2017 al 2019.

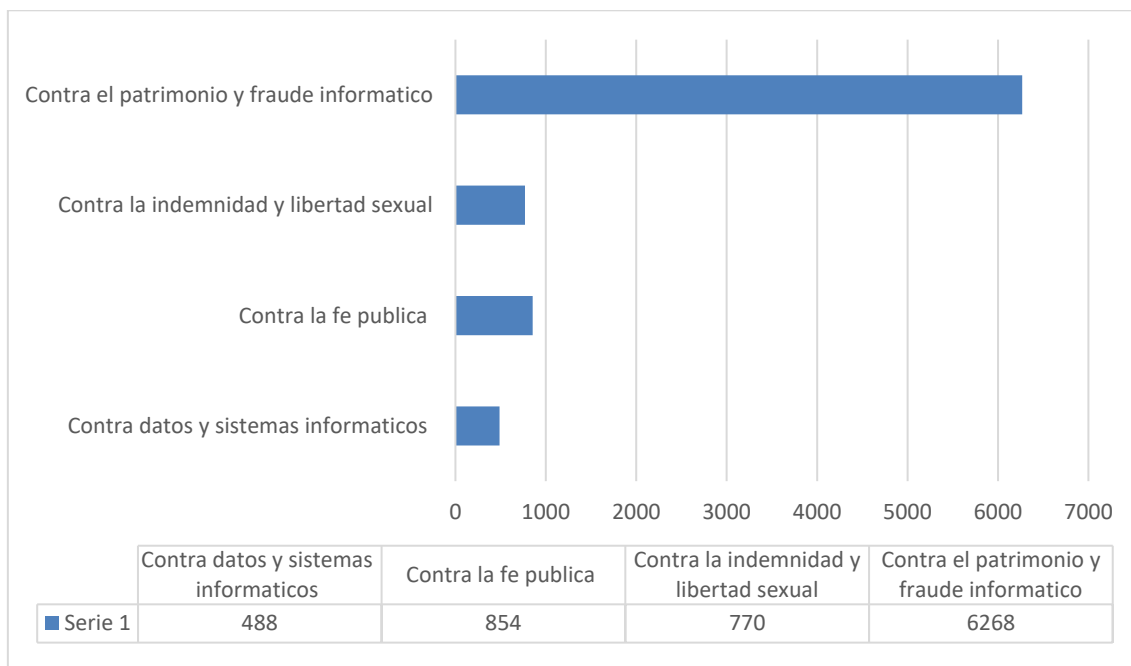


Fuente: Adaptado por el Diagnostico situacional sobre la Ciberdelincuencia en el Perú estadística DIVINDAT- DIRINCRI PNP,2020 recuperado <https://cdn.www.gob.pe/com>

Interpretación: Sobre la información obtenida por la DIVINDAT, cada año aumentan las cifras por delitos cibernéticos. No obstante se han atendido más de 10,110 denuncias que corresponden a delitos informáticos triplicándose anualmente, tenemos que tener en consideración que se debe optar por una mejor infraestructura tecnológica para mejorar el tratamiento de los delitos informáticos protegiendo así la seguridad informática ya que los índices hacen evidencia del crecimiento paulatino de estos ilícitos, considerando que existe normativa internacional para contrarrestar estas no son suficientes para enfréntanos a la ola de criminalidad a nivel nacional.

Figura 10

Análisis de número de denuncias recibidas por la DIVINDAT por tipo de delito.

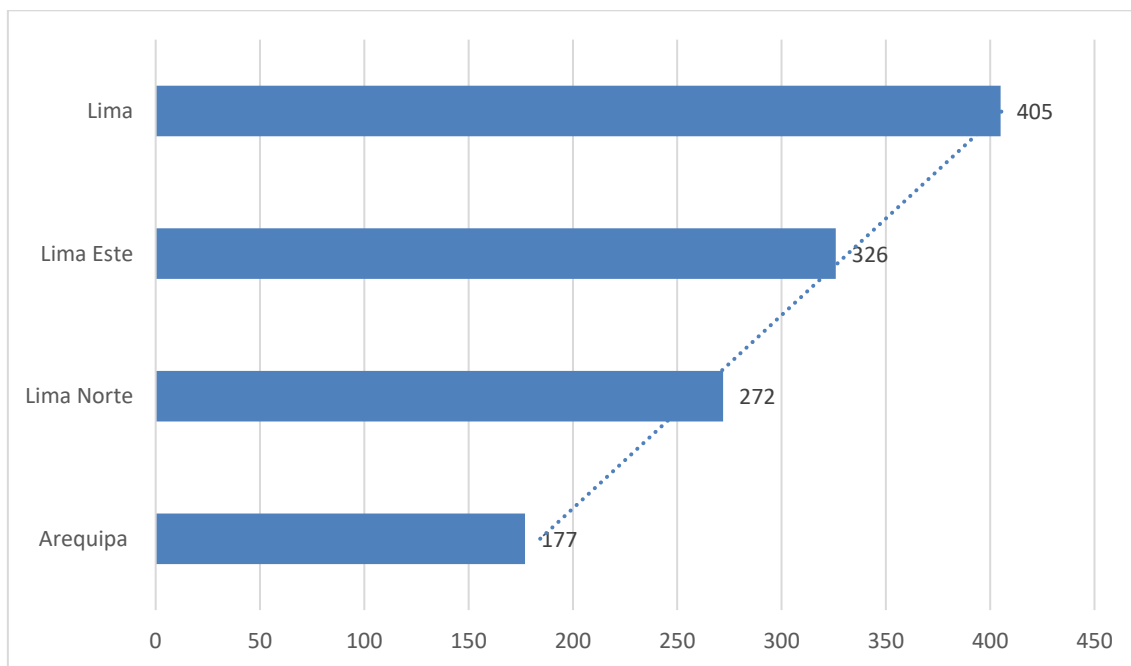


Fuente: Elaboración propia a partir de los datos obtenidos por Diagnostico situacional sobre la Ciberdelincuencia en el Perú estadística DIVINDAT- DIRINCRI PNP.

Interpretación: La información obtenida muestra que el Ministerio Público atendió aproximadamente 4,636 casos sobre delitos informáticos. No obstante, según la información de la PNP, los delitos con más incidencia son contra el patrimonio y fraude informático con un total de 6268 de casos. La comisión de estos delitos son cada día más habituales ya que existe un vacío legal en cuando al encajamiento del acto delictivo y falta de recursos para una investigación preliminar. Posteriormente analizaremos en que distrito fiscal son más recurrentes la comisión de delitos informáticos.

Figura 11

Análisis de casos por delitos contra el patrimonio según distrito fiscal.

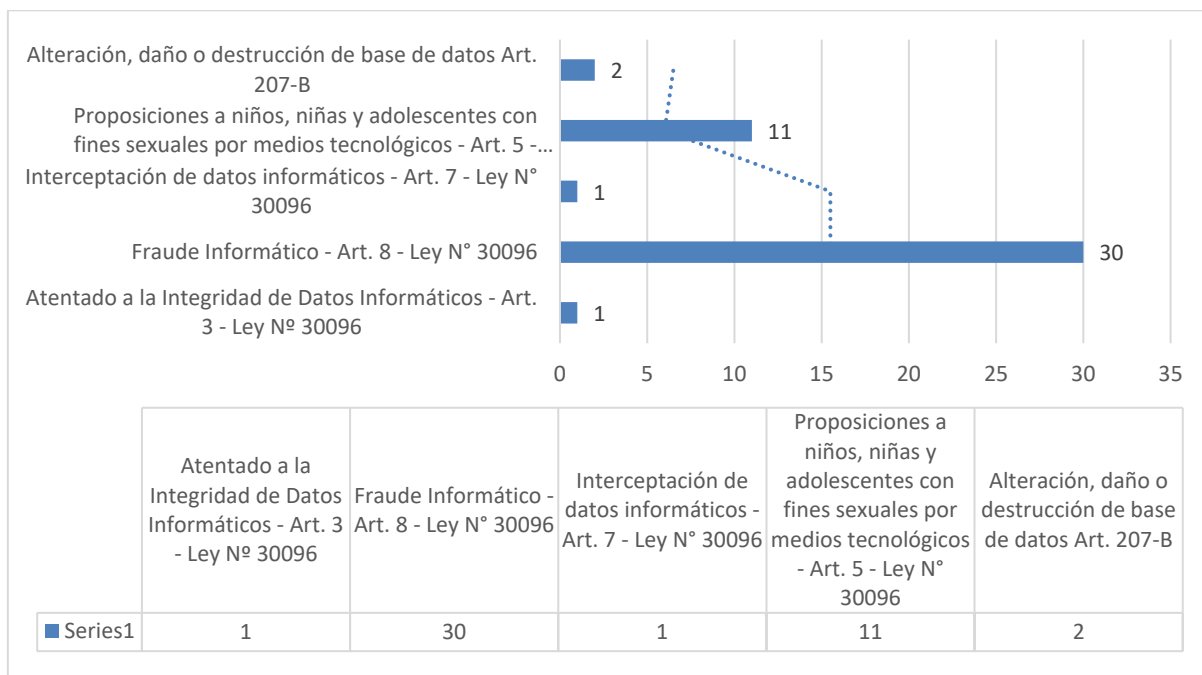


Fuente: Elaboración propia a partir de los datos obtenidos por Diagnóstico situacional sobre la Ciberdelincuencia en el Perú estadística DIVINDAT- DIRINCRI PNP

Interpretación: Según los datos mostrados, hay una mayor incurrencia en determinados territorios como Lima con 405 casos por delitos informáticos, siendo la ciudad con más casos atendidos por los distritos fiscales. Los datos de denuncias son muy significativos, ya que, si bien el Perú tiene varios proveedores privados en servicios de seguridad cibernética, estos no son reflejados en las estadísticas propuestas. Por otro lado, debemos tener en cuenta que el país aún no cuenta con una estrategia nacional de seguridad cibernética, el cual destaca la necesidad de crear una estrategia nacional de ciberseguridad.

Figura 12

Análisis de los casos de delitos informáticos resueltos por el Poder Judicial en el año 2020



Fuente: Elaboración propia a partir de los datos obtenidos por reporte del Poder Judicial.

Interpretación: Según el gráfico mostrado, durante el año 2020 existieron un total de 45 casos atendidos, el cual se ve reflejado en el registro nacional de condenas, con 43 casos sentenciados por la comisión de delitos informáticos regulados en la Ley n.º 30096 y modificatorio n.º 30171. Los casos con mayor incidencia son el fraude informático, atentado a la integridad de datos, y 2 casos con sentencia por la comisión de delitos contra el patrimonio regulado en el artículo 185 al 208 alteración y destrucción de base de datos regulado en el artículo 207-B.

3.3 Resultado del análisis de las entrevistas

Por otro lado, analizaremos los resultados de las respuestas obtenidas por la entrevista a nuestros especialistas, el cual pretende justificar el objetivo de la investigación y las hipótesis planteadas con la finalidad de explicar la importancia de incorporar las modalidades del *phishing*, *smishing* y *vishing* como ilícitos penales.

3.3.1 Análisis de las entrevistas de fiscales y abogados especializados

O.G Justificar por qué los delitos del *phishing*, *smishing* y *vishing* deben ser incorporados en el Sistema Penal como delitos penalizados en el Perú.

1. ¿Considera que los delitos como el *phishing*, *smishing* y *vishing* deben ser incorporados y penalizados en nuestro sistema de justicia?

La Dra. Rodríguez (2020), comenta que sí deberían ser penalizados, por cuanto constituyen las modalidades más utilizadas por los delincuentes informáticos hoy en día para cometer los ciber fraudes. Asimismo, considera que la Ley n.º 30096 posee artículos que carecen de coherencia y genera una confusión al momento de su aplicación por no estar regulados de acuerdo a nuestra realidad social e incluso económica para su aplicación en el ordenamiento jurídico. La norma pretende regular los medios tecnológicos a través de ilícitos penales, pero se olvidan de regular la conducta y busca encajarlo en aquellas conductas que se encuentran establecidas en la normal penal, obviando que estas por su naturaleza deben tener un tratamiento diferenciado. Por ende, debemos tener en consideración que aun el Perú no cuenta con un texto normativo que determine de manera clara los tipos penales, definiendo así los delitos que son cometidos con mayor frecuencia en el mundo digital, la falta de publicidad en cuanto las modalidades, y la carencia procedimientos para sancionar los delitos informativos, además de una falta de cultura informática no solo para los usuarios sino también para agentes de justicia.

A su vez, el Dr. Ramos (2020) comentó que si bien es cierto el Perú cuenta con un gran cuerpo normativo, estos no son suficientes para contrarrestar la ciberdelincuencia; ya que su implementación en el sistema jurídico ha sido deficiente en cuanto a las aplicaciones de mecanismo para imputar el ilícito penal. En la misma línea hace referencia que muchos de los países que se han suscrito al convenio han modificado su legislación, ya que esta debe reflejar la realidad social de cada país, y que la existencia de vertientes pueden inferir a la hora de la imputación del ilícito penal. De igual forma, el Perú hasta el día de hoy no ha previsto este claro vacío debido a que la redacción de la Ley n.º 30096 debido a la similitud al Convenio, además de que la falta de información de los límites de delitos informáticos impide conocer el manejo de determinadas situaciones. En definitiva, es imprescindible mencionar que existe una necesidad de establecer mecanismos para fortalecer la seguridad informática, de modo así crear seguridad en el usuario al momento de este se encuentre conectado en el ciberespacio.

El Dr. Amaya (2020), menciona que la necesidad de la tipificación del *phishing*, *smishing* y *vishing* se sitúa en base a una criminalidad evolutiva de la mano con las nuevas formas de tecnología informática y la comisión de ellas como el empleo de ordenadores que transmiten datos o información. La tipificación de las modalidades mencionadas favorecería al ordenamiento jurídico, ya que individualizaríamos la conducta punible, legislaríamos a partir de una realidad social, más no una realidad mundial, nos adelantariamos a proteger un bien jurídico que muchas otras legislaciones lo han adoptado como la tutela de la seguridad informática, optaríamos por un mejor tratamiento para procesar dichos ilícitos penales, y elevaríamos un mejor nivel de capacitación para los agentes de justicia a no solo tratar delitos tradicionales, si no delitos de alta tecnología.

A su vez, el Dr. Loardo (2020), sostiene que, si bien es cierto la tipificación beneficiaria a la lucha contra la ciberdelincuencia, es necesario reconocer las deficiencias legislativas que posee la Ley n.º 30096 y sus modificatorias en la aplicación actual en sistema legislativo. Primero que no todos los gobiernos provinciales cuentan con la misma información en cuanto a las capacitaciones o el debido procesamiento ante la existencia de denuncias por delitos informativos, y en su mayoría las denuncias registradas tienen mayor incidencia en la ciudad de Lima, pero esto no quiere decir que en provincias no exista la comisión de estos delitos; si no, que muchos de los usuarios que manejan los TIC o no se dan cuenta que han sufrido de algún delito informático o no realizan la denuncia correspondiente. Es por ello que, no se lleva un registro a mayor escala de las denuncias realizadas. No obstante, en su labor como abogado muchas veces ha tenido la oportunidad de observar la falta de peritos en la materia para recaudar pruebas necesarias para la imputación del ilícito penal.

2. En caso que su respuesta fuera afirmativa para penalizar las conductas del Phishing, Smishing y Vishing, ¿cuáles serían los elementos objetivos que deben ser considerados a fin de tipificar dichas conductas?

Por otro lado, Dra. Rodríguez (2020), comenta que, partiendo de las conductas del Phishing, Smishing y Vishing, estas son propias del ciber fraude y aunque el fraude informático como tal está penalizado en la Ley de delitos informáticos en el Perú Ley 30086 y su modificatoria con la Ley 30171.

Elementos objetivos del *phishing*, *smishing* y *vishing*

Sujeto activo: el que “cualquier persona”

Verbo rector: remisión o envío de correo electrónico de manera unitaria o masiva.

Envío de mensajes de texto a través de las TIC, Realización de llamadas telefónicas.

con la finalidad de obtención de datos personales que permitan acceder a sus cuentas

Asimismo, el Dr. Ramos (2020), menciona que la importancia de la tipificación yace de la necesidad de la población de primero informarse sobre las formas de prevención del delito, y así en caso de ser una víctima potencial de este delito es importante conocer la Justicia Penal. Los delitos informáticos siguen siendo un gran problema a nivel mundial debido a una evolución constante y con ello los métodos para cometer delitos también han cambiado con el tiempo.

Sujeto activo: cualquier persona que tenga conocimientos básicos, medios, alto en sistema informático

Sujeto pasivo: Perjuicio de un Tercero

Verbo rector: Interferencia en el funcionamiento del Sistema Informático

Se debe sancionarla afectación de datos informáticos en su interacción con un sistema informático con la finalidad de obtener provecho ilícito en perjuicio de un tercero.

El Dr. Amaya (2020), menciona que, en la tipificación de dichas conductas, lo primero es que proviene de una conducta fraudulenta; es decir, el que engaña al usuario para así obtener datos confidenciales. Segundo, que se basa en el dominio informático que posee el agente activo para la manipulación de los datos. Y, por último, debemos tener en consideración que la finalidad del autor del delito es obtener algún beneficio económico o personal; el objetivo primordial de la tipificación de estos delitos es la necesidad de crear seguridad informática para que todos los que emplean el uso de las TIC tengan plena seguridad que su información estará resguardada.

De igual forma el Dr. Loardo (2020), infiere que los elementos objetivos para tipificar las conductas es la necesidad jurídica de regular aquellas acciones delictivas en nuestra sociedad, también la ineficacia de los agentes de justicia para impartir justicia cuando un usuario ha sido víctima de esta modalidad, la necesidad de actualizar a las instituciones para el tratamiento de los delitos informáticos y la persecución del accionar delictivo.

3. ¿Qué naturaleza jurídica debe adoptar la tipificación de las conductas delictivas del Phishing, Smishing y Vishing, de resultado o de peligro?

La Dra. Rodríguez (2020), considera que tienen que ser delitos de resultado debido que debe concretarse la acción como un efecto del comportamiento humano. Para esto se debe

entender que los delitos de resultado deben estar conectados a la acción; es decir, para que se concrete el delito de fraude informático este debe causar un resultado; es decir, una afectación del bien jurídico protegido por el derecho este debe ser exteriorizado en un determinado espacio geográfico. Por otra parte, el resultado es la plasmación del injusto, es decir la arbitrariedad de la punibilidad de la violación objetiva y subjetiva.

Aunque en otro sentido el Dr. Ramos (2020) asevera que la comisión de los delitos informáticos no encaja en la comisión culposa puesto que el sujeto activo actúa de manera dolosa, ya que conoce y quiere realizar la acción ilícita, puesto que para realizar la manipulación informática es necesario tener un conocimiento básico tecnológico. Ello implica la intención del sujeto activo, ya que sigue un orden lógico para realizar la modificación, alteración de datos y programas. Estas no pueden ser cometidas por error ya que de ahí surge un aprovechamiento económico.

El Dr. Amaya (2020), menciona que la naturaleza jurídica que se debe optar para la tipificación de estas modalidades en el ordenamiento jurídico es de peligro, ya que se perfecciona con sola la realización de la acción del sujeto activo en la perpetuación de la información del sujeto pasivo; de modo que para la comisión del acto es necesario que el agente activo primero tenga conocimientos básicos en ingeniería social para realización de la defraudación. Uno de los criterios subjetivos es que en cuanto la comisión de fraudes informativos o la manipulación de datos es necesario la alteración de los datos o introducción es decir tener conocimientos técnicos para dar pie al perjuicio de un tercero. En relación a esto, el Dr. Loardo (2020) considera que debe ser de resultado por cuanto a la complejidad del tratamiento del delito y su imputación no puede basarse en suposiciones del acto ilícito; si no que este debe concretarse con la producción de un daño. Esta tipificación requiere que el accionar se formalice de manera dolosa.

4. ¿El Perú ofrece programas de capacitación o de información en delincuencia cibernética a la policía, las procuradurías, fiscalías, agentes de la justicia y a la población en general?

La Dra. Rodríguez (2020), señala que sí, pero en su mayoría estas no son completas ya que las capacitaciones no llegan a todos los agentes de justicia. Si bien es cierto que en el 2020 se realizó un taller de investigación criminal y litigación oral especializada en delitos informativos de manera presencial con aproximadamente 50 horas académicas organizada por American Bar Association Rule or Law, así como un curso de investigación Criminal y litigación oral de manera virtual y por ultimo un taller de

ciberdelincuencia, delitos tecnológicos de manera virtual; estos talleres no han beneficiado en su totalidad a los fiscales o especialistas debido a la necesidad de mayor información y publicidad de estos. A su vez, las capacitaciones deben ir de la mano con más presupuesto para obtener instrumentos tecnológicos para combatir la Ciberdelincuencia.

De la misma forma, el Dr. Ramos (2020), señala que en fiscalías de provinciales como la de Huánuco aun no cuentan con capacitaciones sobre delitos informáticos. Además, asevera que las capacitaciones son comúnmente para la zona de Lima; y en efecto para las provincias no llega la publicidad necesaria para optar llevar talleres virtuales. Uno de los comentarios propios que hace el doctor es que existe un descuido por parte del Estado con respecto a las necesidades de las provincias en cuanto a las capacitaciones, o como formalizar las denuncias por delitos informáticos, muy aparte que no cuentan con tecnología apropiada para recaudar los medios probatorios y su mayoría muchos de delitos tradicionales y no tradicionales son llevados a cabo con los recursos que pueden tener a su alcance.

El Dr. Amaya (2020) advierte que si bien es cierto el Perú ha ofrecido capacitaciones en delincuencia cibernética, estas no son completas para desarrollar una cultura informática, ya que no solo es importante que los agentes de justicia se encuentren capacitados, entre ellos el Ministerio Público, el Poder judicial y la Policía Nacional del Perú; si no también los usuarios para que puedan identificar cuando son víctimas potenciales de alguna defraudación informática y las modalidades más recurrentes. Cabe destacar que nos enfrentamos a una realidad virtual creciente que cada día se va perfeccionando, respondiendo a la pregunta si, pero estas no son suficientes para tener una cultura digital ya que requiere de constantes actualizaciones.

Por el contrario, el Dr. Loardo (2020) en su experiencia afirma que en las fiscalías provinciales el estado no se ha preocupado por capacitar a los agentes de justicia debido a que muy pocos de ellos conocen cual es el procedimiento para la persecución del delito, cuando existe denuncias por delitos informáticos, además de no contar con tecnología pertinente, ni agentes especializados, ni pericias sobre dispositivos telefónicos electrónicos de informática, o para determinar dirección IP.

5 ¿Cuáles son las modalidades más frecuentes en el Perú, para la comisión del delito de fraude informático?

La Dra. Rodríguez (2020), menciona que las modalidades más frecuentes para la comisión de delitos de fraude informático son el Phishing, Smishing y Vishing. Estas se computan de la siguiente manera: para empezar el Phishing es un tipo de engaño creado por los hackers con fines delictivos de modo así obtener información confidencial como claves, tarjetas de crédito. Generalmente usan el engaño para la comisión de estos actos delictivos, que se contemplan en la ignorancia del usuario para ingresar a páginas que no son auténticas para proporcionar sus datos. También se consolida usando correos electrónicos de manera masiva para aparentar ser de entidades bancarias de modo obtener información al momento de introducirlos en la página falsa de forma fraudulenta. También tenemos el Smishing, que se utiliza mediante canales digitales diferentes al Phishing como teléfonos celulares, enviado así mensajes de texto donde se falsifica los sitios de entidades bancarias u otras empresas conocidas para así sustraer información personal, o comúnmente que se ha ganado un tipo de premio con un código de validaciones. Todas estas formas delictivas buscan con ello obtener una ganancia económica, además del uso de WhatsApp o Instagram sin la necesidad de proporcionar algún pago si no solamente estar conectado a internet. Por ultimo y no menos importante, también se encuentra el vishing, una técnica muy novedosa que se basa en el uso de la telefonía robotizada donde utiliza el protocolo IP el cual imita las contestadoras automáticas de alguna entidad bancaria para guiarlos así a un número determinado de teléfono o realizando encuestas para robar información confidencial.

Mientras que el Dr. Ramos (2020), sostiene que las modalidades más conocidas y frecuentes en el Perú es el phishing, que es una de las modalidades más usadas por los agentes activos y es el más común ya que se basa en ingeniería social el cual reemplaza la dirección del IP de los servidores para enviar un correo electrónico para poder dirigirlos a una página falsa con la intención de obtener información confidencial con un fin económico. Por otro lado, tenemos al smishing, que usa medios tecnológicos de texto para defraudar a las víctimas induciéndolas a error.

El Dr. Amaya (2020), señala que las modalidades más frecuentes es el phishing y smishing, al cual recurren los denominados Hackers para la comisión de los delitos informáticos como una forma para defraudar a los usuarios induciéndoles en error y así robar información confidencial para luego obtener un beneficio económico.

Necesariamente para que el agente activo robe información es necesario que este tenga conocimientos técnicos para la realización de hecho punible.

Asimismo, el Dr. Loardo (2020) afirma que los delitos más recurrentes son los fraudes cibernéticos, por cuanto la comisión de este hecho puede resultar provechosa para los delincuentes debido a que por su naturaleza hace más difícil la persecución del delito, sacando provecho así a esta situación, debido a que los perpetuadores tienen seguridad de que rastrearlos será dificultoso para la DIVINDAT; es más, incluso muchos de los usuarios no realizan las denuncias pertinentes por un tema de tiempo, o que el monto económico no es significativo.

6 Desde la adhesión al Convenio de Budapest 2019 y la Ley n.º 30096, ¿El Perú ha podido minimizar los casos de Delitos informáticos?

La Dra. Rodríguez (2020) considera que no, ya que el Convenio de Budapest tiene como fines que los países miembros tengan una legislación óptima en delitos informáticos y busca una colaboración rápida y eficaz entre los países miembros. Sin embargo, la legislación sobre delitos informáticos “Ley n.º 30096 y su modificatoria Ley n.º 30171” así como las modificaciones que se le han hecho a diferentes tipos penales para incluir su comisión a través de las TIC no han sido suficientes para minimizar la comisión de los mismos. Debe tenerse presente que en la actualidad los delincuentes van creando nuevas modalidades delictivas haciendo uso de las TIC, lo cual genera que se puedan obtener muchas modalidades que vayan perfeccionándose en el tiempo.

De igual forma, el Dr. Ramos (2020) sostiene que en el periodo del 2019 recibieron un total de 3012 denuncias por casos de delitos informáticos y a pesar de contar con normativa para el tratamiento de estos delitos, no han sido suficientes para combatir la ciberdelincuencia ya que, en concordancia con la Dra. Rodríguez, los delincuentes van creando nuevas modalidades de manera sofisticada para perpetuar la comisión de los ilícitos penales. También menciona que debemos tener en consideración que existe muchos factores que posibilitan la comisión de estos delitos, como por ejemplo falta de capacitaciones para los agentes de justicia, no contar con una adecuada información para el procesamiento y la recaudación de pruebas de estos delitos, no contar con tecnología sofisticada para evitar su perpetuación. y que no contamos con un plan de protección de la seguridad informática.

El Dr. Amaya (2020), en su opinión, menciona que no siempre la creación de normas de manera masiva va erradicar el problema de la delincuencia informática o tradicional. Esto

se va ir perfeccionando en cuanto a las necesidades que recae en la implementación, como un presupuesto designado para que los agentes de justicia y que tengan mecanismos para obtener las pruebas para la imputación del delito, es decir tecnología altamente sofisticada para la persecución del delito, capacitación para el debido procesamiento del delito. Muchos de estos factores influyen para que la implementación de las leyes sea viables o eficientes, pero partiendo de la necesidad del encajamiento de la conducta penal, considera que es nacería la tipificación ya que denota la existencia de una incertidumbre de la población a la hora de manejar los TIC, es por ello la necesidad de proteger la seguridad informática.

En concordancia, el Dr. Loardo (2020) sostiene que se supone que, con la creación de normas para proteger bienes jurídicos e impartir justicia a la sociedad, estas deberían ser eficaces no solo en cuanto a la estructura normativa si no en su implementación. Viéndolo así, esta no es la realidad del Perú ya que poseemos muchas leyes y no todas son aplicadas correctamente. El doctor Loardo, como apreciación propia, sostiene que el estado debería preocuparse no por la creación de normas, sino porque cada una tenga una debida implementación y que los mecanismos, ya sea educativos y económicos, lleguen de manera igualitaria a nivel nacional, y que los agentes de justicia estén siempre a la vanguardia de la realidad social, y no esperar la perpetuación del bien jurídico para crear normativa necesaria para sociedad.

7 ¿Existe hoy en día para los operadores de justicia alguna dificultad para la investigación y recaudación de prueba?

La Dra. Rodríguez (2020), menciona que sí, entre las dificultades tenemos:

Falta de capacitación especializada en delitos informáticos tanto para magistrados, abogados y peritos, y la mayor dificultad es la obtención de información de un elemento electrónico , como la dirección del IP y habilitar la clave de teléfonos bloqueados, no contar con peritos informáticos en el Ministerio Publico para acelerar el proceso de investigación y que en muchos casos si se trata de provincias estas tiene que remitirlas en la ciudad de Lima para recién alguna fuente relevante para la investigación. Cabe señalar que una de las dificultades para el enjuiciamiento de los delitos informáticos es que en muchos casos no se logra identificar al autor, y sobre todo la falta recursos para la contratación de personal especializado, logística, etc.

De modo similar, el Dr. Ramos (2020) sostiene que sí, existe dificultades para la investigación y la recaudación de las pruebas, ya que muchas fiscalías provinciales

incluso no cuentan con equipos con alta tecnología para poder primero identificar al autor, y es curioso que incluso los ciberdelincuentes cuenten con mejor tecnología para perpetuar el daño que el mismo estado para defender el bien jurídico. La falta de capacitación de la Policía Nacional del Perú en uso de técnicas de investigación especiales y la falta de pericias, así como la falta de la tipificación del delito del *phishing*, *smishing* y *vishing* impiden combatir la delincuencia en el Perú, ya que estaríamos creando mecanismos para el encajamiento de la conducta típica en el ordenamiento jurídico teniendo en consideración que esta necesidad subyace de que su accionar no es estático y con el tiempo se va ir perfeccionando la comisión de estos delitos.

El Dr. Amaya (2020), considera que se debe tener en cuenta medios tecnológicos innovadores para la obtención de pruebas necesarias para la imputación del ilícito penal; primero porque haciendo un análisis este conlleva a un vínculo de causa-efecto, debido a que el perpetuador puede encontrarse en el anonimato, y la facilidad para encubrirse mediante ordenadores y así ocultar la dirección de su IP “dirección del protocolo de internet”. Otro punto para tomar en consideración es el espacio geográfico, ya que por medio de los ordenadores no siempre el delincuente se encuentra en el lugar de los hechos; y para finalizar, si bien es cierto los TIC están a disposición de muchas personas, se necesita de conocimientos básicos para cometer el ilícito penal y a su vez de una policía técnica especializada que cuenten con todos los mecanismos tecnológicos para la persecución del delito.

Por su parte, el Dr. Loardo (2020) señala que existen dificultades y realidades diferentes, debido a que, si comparamos la realidad socioeconómica de Lima y las provincias, estas son abismales, puesto que al no contar con una Unidad de Alta Tecnología de la Policía Nacional al igual que Lima, ni con peritos informáticos del Ministerio Público, genera demoras en la investigación, ya que tiene que remitir las pruebas a la ciudad de Lima para que estas sean investigadas en la ciudad de origen.

8 ¿Existe un incremento anual de los Delitos informáticos?

La Dra. Rodríguez (2020), afirma que sí; los delitos informáticos en general han aumentado sobre todo en la época de la pandemia donde debido a la cuarentena y a las restricciones producto de la COVID 19, los delincuentes también han optado por estas nuevas formas de ciber criminalidad. Según las denuncias por delitos informáticos investigados por la DIVINDAT, entre el periodo del 2017 hay una incidencia de 1219 denuncias y en el 2020 hay un aumento de 9515 denuncias. Hasta aquí podemos analizar

que el incremento anual es significativo y cada vez existe más modalidades para defraudar a los usuarios.

Como contrapartida, el Dr. Ramos (2020) sostiene que sí, existe un incremento progresivo de la comisión de Delitos informáticos. Este ha tenido mayor incidencia en la pandemia ya que como nos sometimos a una nueva realidad social que es la inmovilización nacional, se optaron por nuevas formas para realizar tareas cotidianas, como el trabajo remoto haciendo posible mediante la utilización de los TIC, las compras virtuales de insumos básicos, o incluso las ventas de productos y la publicidad de ellos. Esto nos hizo denotar las deficiencias legislativas en cuanto a la protección de los usuarios en el mundo digital y la falta de creación de mecanismos que protejan la seguridad informática o de la información. Se debe considerar que aun muchos de los usuarios desconocen que existe herramientas y mecanismos para evitar ser víctimas del *phishing*, *smishing* y *vishing*, aun cuando se ha visto la necesidad que estas estén contempladas en el ordenamiento jurídico. Por el contrario, las víctimas no suelen denunciar estos delitos debido a que no todos tienen la información necesaria de que se trata estas modalidades.

El Dr. Amaya (2020) señala que si existe un crecimiento significativo de los delitos informáticos. Cada vez vemos a más víctimas que han sufrido alguna de estas modalidades de defraudación, incluso en las noticias estos hechos son cada vez más comunes.

Asu vez, el Dr. Loardo (2020) sostiene que existe un periodo de crecimiento de los delitos informáticos, pero considera que este se ha prolongado durante el 2020 donde se ha podido aprovechar más el uso de los TIC. Cabe resaltar que los usuarios durante este periodo han tenido como única forma de comunicarse con sus familiares, a través de las redes sociales, cuando aparece realidades diferentes en nuestra sociedad genera necesidades normativas, hace 10 años atrás no nos imaginamos que alguien pueda cometer un delito o defraudación a la través de las computadoras, hoy en día es una problemática social.

9 ¿Cuáles son delitos informáticos más recurrentes durante el periodo del 2020?

La Dra. Rodríguez (2020), Conforme el Informe de análisis N.º 04 – Ciber delincuencia en el Perú: pautas para una investigación fiscal especializada elaborado por el Ministerio Público y OFAEC “Oficina de análisis estratégicas contra la criminalidad”, brinda

información en los siguientes rubros entre los años 2013 – 2020 los delitos que tienen más incidencia con un 78.5% son los delitos informáticos

En otro sentido el Dr. Ramos (2020). menciona que en la provincia de Huajuco no denota mucha incidencia en cuanto a las denuncias por delitos informáticos considera que el punto de auge se encuentra en la ciudad de Lima. No obstante, el hace mención de que las personas que han sido víctimas de estos ilícitos penales o no tienen conocimiento de que pueden denunciarlos o advierten que sería una pérdida de tiempo debido a que en su mayoría no ha sido un monto significativo. Pero haciendo una valoración propia si juntamos el número de usuarios que han sido víctimas de estos delitos dados solo por un perpetuador, el monto ascendería considerablemente. De igual forma, el estado debe proteger aquellos vacíos legales frente a una sociedad cambiante en este caso hablamos de la protección de la seguridad informática.

El Dr. Amaya (2020) señala que los delitos más comunes son el fraude informático y la suplantación de identidad, cuya incidencia ha tenido mayor relevancia en el periodo del 2020 debido a las medidas sanitarias dispuestas por el presidente del Perú; de modo tal que nos ha sacado al descubierto las deficiencias legislativas en cuanto a la implementación de la Ley n.º 30096.

En concordancia, el Dr. Loardo (2020) afirma que los delitos más recurrentes son los de Fraude informático, y que este se intensifico con la llegada de las medidas sanitarias. Uno de los elementos que se debe considerar es el uso masivo de diferentes plataformas de interacción virtual. Señala que la necesidad se sitúa en creación de normas que protejan la seguridad informática, ya que cada día existe más usuarios que pueden ser considerados como potenciales víctimas incluso las que usan plataformas de juegos o streaming. Por eso, la iniciativa de crear mecanismos de protección de la seguridad informativa es importante adaptarla en el Perú y la constante capacitación y actualización permanente de los agentes de justicia.

Análisis a la entrevista al efectivo de la DIVINDAT

1. ¿Considera que la DIVINDAT cuenta con los recursos logísticos suficientes para atender las denuncias a nivel nacional?

Leiva (2020), menciona que cuentan con departamentos de investigación de delitos informáticos y la DIVINDAT para que atienda temas de logística a nivel nacional, pero estas no son suficientes, ya que la comisión de delitos informáticos se perpetua a nivel nacional. Si bien es cierto que existe la DIRINCRI, esta unidad sirve para atender casos

de menor complejidad; no obstante, afirma que el estado debe proporcionar capacitaciones actualizadas y proporcionar tecnología innovadora para que sea más eficiente la persecución del delito. Por otro lado, la DIVINDAT es una Unidad Especializada en tratar casos vinculados a delitos informáticos, es por ello que es importante que muchas de las víctimas sepan que existe unidades especializadas donde se pueden realizar las denuncias y no generar incertidumbre por la imputabilidad del derecho vulnerado, la necesidad publicidad con respecto a que delitos atiende la DIVINDAT y cómo evitar ser víctimas potenciales de un fraude informático.

2. ¿A qué se debe el incremento anual de los delitos informáticos?

Leiva (2020) señala que este se ha incrementado durante el periodo del 2013 ya que se empezó a utilizar con más frecuencia los TIC, y la aparición de plataformas sociales para la intercomunicación digital. Asimismo, la aparición de nuevas modalidades de defraudación, si bien es cierto muchos de los bancos han tratado de mejorar la seguridad en sus plataformas digitales, todavía tenemos un factor social que influye mucho que es la falta de educación informática, ya que si bien representa un beneficio para realizar tareas cotidianas también puede ocasionar daños y no solo económicos porque con la masificación de los delitos informáticos podemos ver que el robo de información crea incertidumbre.

3. ¿Considera que es importante la tipificación de las modalidades como el Phishing, Smishing y Vishing en nuestro ordenamiento jurídico?

Leiva (2020), afirma que la tipificación en nuestro sistema penal ayudaría a generar mecanismos que protejan la seguridad informática, de modo que son las modalidades más comunes para la comisión de delitos de fraudes informáticos. Esto debe ir de la mano con capacitaciones a nivel nacional; muchas provincias se encuentran desorientadas cuando se trata del procesamiento correcto de delitos informáticos y por ende recae la acusación.

3.4 Resultados del análisis de la legislación

Para el desarrollo del trabajo se realizó un breve análisis de las leyes más relevantes de los delitos informáticos con la finalidad de evaluar si es necesario la incorporación del *phishing*, *smishing* y *vishing* como delitos penalizados en nuestra legislación, es por ello que se ha realizado tablas con el fin de tener una mejor visualización del tema propuesto.

Tabla 4

Evolución de la creación normativa sobre los Delitos Informáticos

LEY	FECHA DE PRESENTACION	TITULO
Código Penal de 1991	17/07/2000	Artículo 186, inciso 3 No se consideraba como un delito autónomo, si no como una agravante del delito de Hurto, Artículo 185.
Ley N°30096 Ley de Delitos Informáticos	22/10/2013	Capítulo I delitos contra datos y sistemas financieros Capitulo II delitos informáticos contra la indemnidad y libertad sexual Capitulo III delitos informáticos contra la intimidad y secreto de las comunicaciones Capitulo IV delitos informáticos contra el patrimonio Capitulo delitos informáticos contra el patrimonio Capitulo V delitos informáticos contra la fe publica Capítulo VI disposiciones comunes
Ley N°30171 (Ley que modifica la Ley N°30096)	10/03/2014	Tiene como finalidad adecuar la Ley N°30096 a los estándares legales del convenio sobre cibercriminalidad (Convenio de Budapest incorporar los artículos 2,3,4,7,8 y 10)

Fuente: Elaboración propia a partir de los datos obtenidos por informe del Poder Judicial- Tratamiento del Ciberdelito

A lo largo del tiempo, el país se vio en la necesidad de incorporar delitos informáticos en el ordenamiento jurídico; se logró incorporar en el Título V correspondiente a los delitos contra el patrimonio, el delito informático en el artículo 207-A, el delito de alteración, daño y destrucción de base de datos, sistema, red o programas de computadoras en el artículo 207 y el delito informático agravado en el artículo 207 para así erradicar la ciberdelincuencia en el Perú

El fenómeno de la globalización se caracteriza principalmente por el crecimiento mundial de los TC razón por la cual que juega un papel muy importante en la sociedad y el desarrollo de la cultura simplificando las tareas cotidianas como el teletrabajo, las compra y venta y la interacción digital, cuyo objetivo es procesar y almacenar datos en tiempo récord, herramientas como el correo electrónico, WhatsApp, Facebook, Instagram que están siendo implementada como parte de un gobierno digital.

No obstante tiempo después se crea la ley de delitos informáticos desarrollada en concordancia con el convenio de Budapest, en la cual se detalló la estructura legal de la norma dándole así una distribución normativa, que a continuación analizaremos.

Tabla 5

Ley de Delitos informáticos

DELITOS INFORMATICOS				
Capitulo II	Capitulo III	Capitulo IV	Capitulo V	Capitulo VI
Delitos contra datos y sistemas informáticos	Delitos informáticos contra la indemnidad y libertad sexual	Delitos informáticos contra la intimidad y el secreto de las comunicaciones	Delitos informáticos contra el patrimonio	Delitos informáticos contra la fe pública
Art. 2 Acceso ilícito: Art. 3 Atentado contra datos Art. 4 Atentado contra sistemas informáticos	Art.5 Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos: El que, a través de las tecnologías de la información o de la comunicación, contacta con un menor de 14 para solicitar u obtener de él material	Art. 7 Interceptación de datos informáticos El que, a través de las tecnologías de la información o de la comunicación, intercepta datos informáticos en transmisiones no públicas, dirigidas a un sistema informático,	Art. 8 Fraude informático Este tipo penal sanciona la acción de introducir, diseñar, borrar, suprimir, alterar y clonar información cibernética, perjudicando a una tercera persona, y es considerado	Art. 9 Suplantación de identidad El que, mediante las tecnologías de la información o de la comunicación suplanta la identidad de una persona natural o jurídica, siempre que de dicha conducta resulte algún perjuicio,

	<p>pornográfico, o para llevar a cabo actividades sexuales con él, será reprimido con pena privativa de libertad no menor de 4 ni mayor de 8 años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal. Cuando la víctima tiene entre catorce y menos de 18 años de edad y medie engaño, la pena será no menor de 3 ni mayor de 6 años e inhabilitación conforme a los numerales 1, 2 y 4 del artículo 36 del Código Penal</p>	<p>originadas en un sistema informático o efectuadas dentro del mismo, incluidas las emisiones electromagnéticas provenientes de un sistema informático que transporte dichos datos informáticos, será reprimido con pena privativa de libertad no menor de 3 ni mayor de seis años. La pena privativa de libertad será no menor de 5 ni mayor de ocho años cuando el delito recaiga sobre información clasificada como secreta, reservada o confidencial de conformidad con las normas de la materia</p>	<p>como un delito de resultado toda vez que para su consumación se requiere que la acción cometida por el sujeto activo perjudique a un tercero o genere un beneficio para sí mismo</p>	<p>material o moral, será reprimido con pena privativa de libertad no menor de 3 ni mayor de 5 años</p>
--	---	---	---	---

Fuente: Elaboración propia a partir de los datos obtenidos por la Ley N°30096- Ley de Delitos informáticos

No obstante, debemos tener en consideración que la actual regulación de los delitos informáticos cuenta con bastante similitud en cuanto a la redacción del convenio de Budapest, tratado internacional sobre la ciberdelincuencia que tiene como finalidad hacer frente a la criminalidad informática a través de mecanismos de homologación aplicar los estándares de procesos penales y cooperación internacional. El Perú cuenta con una

Unidad de Cooperación judicial Internacional y Extradiciones con el objetivo de facilitar la confrontación de delitos que traspasen los límites geográficos.

Por otro lado, podremos analizar uno de los aspectos más relevantes de nuestra tesis la protección la seguridad informática puesto a disposición mediante el proyecto de Ley 5630/2020 “Ley de seguridad informática y represión de los delitos informáticos” por la congresista Robertina Santillana Paredes por el grupo parlamentario de Alianza por el Progreso, a continuación, realizaremos una tabla para un mejor entendimiento.

Tabla 6

Ley de seguridad informática y represión de los delitos informáticos

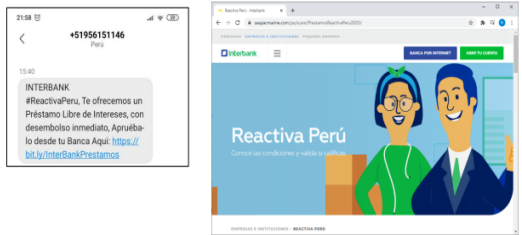

Ley 30096	Propuesta	Comentario
<p>Artículo 1. Objetivo de la Ley</p> <p>Tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidos mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia.</p>	<p>Artículo 1. Objeto de la Ley</p> <p>El objeto de la presente ley es establecer</p> <p>1.1 Establecer reglas de seguridad informática de aplicación en el Estado Peruano</p> <p>1.2 Impulsar el Comercio electrónico y proteger al consumidor del mismo.</p> <p>1.3 Dar cumplimiento a la obligación de adecuar la Ley de Delitos Informáticos a lo dispuesto por el Convenio sobre la Ciberdelincuencia adoptado en Budapest, el 23 de noviembre del año 2001, aprobado con reservas por el Estado Peruano mediante la Resolución Legislativa N°30913, publicada el 13 de febrero de 2019 en el diario oficial.</p>	<p>El Proyecto tiene la finalidad pues da pie a tres necesidades básicas.</p> <p>1.1 Mejorar las reglas de seguridad en el Estado Peruano</p> <p>1.2 Establecer un estándar mínimo de protección para el consumidor de bienes y servicios por medios tecnológicos</p> <p>1.3 Cumplir con adecuar la legislación nacional a lo preceptuado por el Convenio de Budapest como normal legal en el Perú</p>

Fuente: Proyecto de Ley 5630/2020 -Ley de seguridad informática y represión de los delitos informáticos por la congresista Robertina Santillana Paredes

Posteriormente, se realiza el análisis de la estructura orgánica de la PNP con respecto a las modalidades delictivas del *phishing* y *smishing* y el actuar delictivo para la comisión del ilícito penal. No obstante, es necesario señalar que los esfuerzos por combatir la criminalidad informática no son suficientes, ya que nos enfrentamos a una era digital progresiva. Por otro lado, debemos destacar la ardua labor que realiza la DIVINDAT para combatir los delitos informáticos aun cuando la tecnología que posee no sea la mejor para la persecución de ilícito penal.

Tabla 7

Modalidades delictivas SMISHING y PHISHING, suplantando la identidad a entidades Bancarias.

EXTRUCTURA ORGANICA	MODALIDADES DE DEFRAUDACION
<p>La División de Delitos de Alta Tecnología, cuenta con el Departamento de Patrullaje Virtual, encargado de realizar las búsquedas de información en Internet y redes sociales con la finalidad de ubicar, identificar e informar a la unidad policial competente sobre alguna actividad ilícita que venga haciendo uso por medio de los TIC.</p>	
<p>Se encarga de atender pedidos de búsqueda de información proveniente de las diferentes subunidades del Sistema de Investigación Criminal, Unidades Policiales, Ministerio Público, Poder Judicial y Órganos de Control PNP (IG PNP) a nivel nacional.</p>	

Fuente: Informe de la policía nacional del Perú dirección de investigación criminal división de investigación de delitos de alta tecnología n 113-2020

En definitiva, de los resultados obtenidos en el análisis documental, las entrevistas, la doctrina nacional, así como de la legislación nacional, se detectó que nuestro sistema de justicia vigente resulta inapropiado para realizar el procesamiento de la comisión de los delitos informáticos normados en la Ley n.º 30096 y la Ley n.º 30171, así como los delitos informáticos.

A su vez la importancia de sancionar el *phishing*, *smishing* y *vishing* es debido a que el delito cibernético ocupa un lugar muy importante en la sociedad. La idea de generar educación informática para la prevención del delito. Si bien es cierto que contamos con

normativa para esta clase de delitos, el estado no ha previsto la idea de proteger la seguridad informática; la tecnología es evolutiva y con ello las formas de impartir justicia y los métodos para cometer esos delitos también cambian. Por ello, es necesario enriquecernos con herramientas jurídicas que generen seguridad al momento de realizar transacciones realizadas por medio electrónicos. El empleo se sitúa en combatir nuevos fenómenos tecnológicos en lo que respecta el derecho penal sustantivo como la interceptación de la comunicación a través de la tecnología VOIP “Voz sobre Protocolo de Internet”⁴, la admisión de pruebas digitales o la investigación de casos que se han utilizado la tecnología de cifrado.

Para terminar, el análisis realizado por medio de las entrevistas nos muestra que muchos de los agentes de justicia concuerdan que la investigación de delitos cibernéticos es de mucha complejidad, sobre todo al momento de enjuiciar a las personas involucradas. Es por eso que debe realizarse capacitaciones actualizadas a los jueces, abogados y población y una debida publicidad de delitos informáticos. Mi tesis pretende justificar por qué es importante tipificar las modalidades mencionadas para así cubrir los vacíos legales de acuerdo a las necesidades de una sociedad cambiante, estableciendo normas en relación de la prevención del delito y la impartición de justicia penal.

⁴ VOIP: significa voz a través de internet es una tecnología que proporciona la comunicación de voz y sesiones multimedia tales como vídeo sobre Protocolo de Internet (IP).

CAPÍTULO IV. DISCUSIÓN Y CONCLUSIONES

4.1 Discusiones

4.1.1 Limitaciones

En este trabajo se propone, según lo recopilado en los capítulos anteriores, la descripción de las limitaciones en función de las hipótesis plasmadas para el estudio y análisis del trabajo de investigación. Esta se va dividir en dos vertientes, principalmente con relación a los límites que se tuvo para afrontar la posición como la viabilidad de las fuentes y los recursos económicos, y en segundo lugar las limitaciones propias de la investigación los recursos humanos y la viabilidad de la propuesta planteada mediante el cual se expusieron en los siguientes párrafos.

4.1.1.1 Limitaciones del autor

En cuanto a las limitaciones solo pudimos realizar entrevistas a especialistas en el ámbito nacional, de modo que no se ha podido acceder a entrevistas de expertos extranjeros, que tuvieran basta experiencias en la criminalidad informática el cual hubiera ayudado mucho a la investigación, ya que en el Perú hay pocos especialistas que tengan conocimientos plenos en delitos Informáticos

Con respecto a la viabilidad de la investigación se puede decir que la información encontrada se encuentra contenida en los repositorios de las universidades nacionales y extranjeras, noticias, páginas web internaciones. Es importante resaltar que aun el Perú carece de información complementaria que pueda absolver muchas dudas con respecto a los delitos informáticos. La mayoría de la información fue encontrada en tesis internacionales, de lo que se desprende la carencia de material de investigación en sede nacional.

Para finalizar, con respecto a las cuestiones económicas para la investigación estas tuvieron un aporte considerable ya que realizo una pequeña conferencia sobre la cibercriminalidad en el Perú cuyo ponente fue el Dr. Elías Puelles, presidente del Observatorio Peruano de Cibercriminalidad, además de la compra de un libro digital sobre la Cibercriminalidad cuyo fin es ayudar a extensivamente a la investigación.

4.1.1.2 Limitaciones de la investigación

La investigación se realizó tomando en cuenta la Ley n.º 30096 y su modificatoria Ley n.º 30171 Ley de Delitos Informáticos, convenio de Budapest, información del

Observatorio Peruano de Cibercriminalidad, reportes de la ciberseguridad propuesto por la OEA 2019-2020; no obstante, cabe mencionar la carencia de información actual sobre delitos Informáticos.

La falta de estudios previos de investigación sobre el tema y la escasez de fuentes bibliográficas especializada en delitos informáticos, la construcción de los antecedentes, marco teórico fue necesario recurrir (artículos, consultas web, especialistas en delitos informáticos, revistas, noticias) para poder obtener material bibliográfico para la investigación y la falta de datos disponibles y/o confiables y la carencia de manejo de vocabulario técnico con respecto al tema, ya que es propia de Ingeniería informática especializada en medios tecnológicos como el RAW, Shellcode, firewall, sistema operacional, Spam, Proxy, malware⁵.

4.1.2 Interpretación comparativa

Para este apartado se realizó la discusión de los resultados tomando la información del análisis de las entrevistas, documentos y la legislación, esto ha permitido interpretar los estudios realizados con anterioridad, como la conexión de los objetivos y las hipótesis de la investigación, realizándose con la finalidad de proponer un beneficio para la comunidad y crear normativa que asegure la protección de bienes jurídicos supraindividuales.

O.G Justificar por qué los delitos del phishing, smishing y vishing deben ser incorporados en el Sistema Penal como delitos penalizados en el Perú.

H.G Las modalidades delictivas del phishing, smishing y vishing no se encuentran reguladas en la legislación peruana, en ese sentido, a la fecha existe cierta impunidad de estas conductas.

⁵ RAW: Entiéndase como "en crudo" siguiendo el término anglosajón para denominar a los brutos de cámara.

Shellcode: Es un conjunto de órdenes programadas generalmente en lenguaje ensamblador y trasladadas a opciones de ejecución de un programa para conseguir que la máquina en la que reside se ejecute la operación que se haya programado.

Firewall: Son programas de software o dispositivos de hardware que filtran y examinan la información que viene a través de su conexión a Internet.

Sistema operacional: Es un conjunto de programas que permite manejar la memoria, disco, medios de almacenamiento de información y los diferentes periféricos o recursos de nuestra computadora

Spam: Es correo basura digital comunicaciones no solicitadas que se envían de forma masiva por Internet o mediante otros sistemas de mensajería electrónica.

Proxy: Es una red informática, es un servidor programa que hace de intermediario en las peticiones de recursos que realiza un cliente a otro servidor.

Malware: Se llama programa malicioso, programa malintencionado, o código maligno, a cualquier tipo de software que realiza acciones dañinas en un sistema informático de forma intencionada y sin el conocimiento del usuario.

Sobre la tipificación del *phishing*, *smishing* y *vishing* en nuestro Sistema Penal Peruano

Una de las razones que conllevarían a la tipificación de las modalidades delictivas mencionadas es debido a que muchas de estas actividades atentan contra el sistema informático y violentan las garantías de la seguridad en la red. Esto se ha dado a conocer con más frecuencia durante los periodos 2018 en adelante debido a un uso más prolongado de los TIC. Estas modalidades, como el *phishing*, *smishing* y *vishing*, se computan mediante el uso de la tecnología. Tal es así que no se encuentran regulados en la legislación peruana; es decir, existe una necesidad de regular dichas actividades ya que son las modalidades más frecuentes en el mundo informático. Es por ello que debemos tener en cuenta que el uso del internet se ha convertido en una herramienta de mayor relevancia al momento de realizar tareas cotidianas; sin embargo, al no encontrarse regulado en nuestro sistema penal, no podríamos configurarlo al momento de realizar la persecución del delito. Por lo tanto, penalizar dichas conductas con pena privativa de libertad reduciría los índices de ciberdelincuencia. Cabe resaltar que es muy importante realizar una valoración económica de los ilícitos generados en el sistema informático; es decir, determinar si la conducta se configura como una infracción administrativa o comportamiento penal y la gravedad de estos delitos en nuestra sociedad, y la poca importancia que le damos al momento de la persecución del delito teniendo en cuenta nuestra realidad social.

Por otro lado, debemos tener en consideración que a pesar de que contamos con la Ley de Delitos Informáticos n.º 30096 y su modificatoria Ley n.º 30171, estas no son suficientes para enmarcar todas las conductas delictivas que enfrenta nuestro país y realizar una correcta persecución del delito y así evitar la impunidad de ella. Tal como lo muestra las cifras con durante el periodo del 2013 y 2020 se recibió un total de 23,657 denuncias, con un 58% (12608) de denuncias que han sido archivadas y un 41% (8842) que se encuentran en proceso de investigación, haciendo referencia que muchos de los casos de delitos informáticos no llegan a la imputación de la pena debido a que existe algunas deficiencias en el proceso de la investigación, dando claras luces que nuestro actual sistema de justicia resulta inapropiado para el procesamiento de estos delitos.

A su vez, los doctores Rodríguez, Ramos y Amaya (2020) consideran que sí deberían ser penalizados, por cuanto constituyen las modalidades más utilizadas por los delincuentes

informáticos hoy en día para cometer los ciber fraudes. No obstante, considera que la Ley 30096 posee artículos que carecen de coherencia y genera una confusión al momento de su aplicación por no estar regulados de acuerdo a nuestra realidad social. En ese sentido, hace referencia que muchos de los países suscritos al convenio de Budapest han modificado su legislación, ya que esta debe reflejar la realidad social de cada país, ya que la existencia de vertientes puede inferir a la hora de la imputación del ilícito penal. Por otra parte, el Perú hasta el día de hoy no ha previsto este claro vacío debido a que la redacción de la Ley n.º 30096 es muy similar al convenio de Budapest; además de que la falta de información de los límites de delitos informáticos impide conocer el manejo de determinadas situaciones.

Para concluir, al tratarse de modalidades que pueden ocasionar daños, debe existir una adecuada publicidad para la prevención del delito. Si bien es cierto que es una problemática compleja en cuanto a su tratamiento, debido a que la tecnología es evolutiva y no estática a diferencia de los delitos tradicionales, se deben elaborar soluciones para evitar la impunidad del delito, ya que también los métodos utilizados para su comisión cambian.

Sobre la impunidad de las modalidades delictivas del *phishing*, *smishing* y *vishing* debido a que no se encuentran reguladas en la legislación peruana

Con respecto a la impunidad de las modalidades delictivas, debe considerarse que estas han tenido una mayor incidencia en el año 2020, probablemente por el uso frecuente de medios tecnológicos para realizar actividades tanto laborales como comerciales. Al no encontrarse regulado estas modalidades, tienen gran repercusión en los derechos de los usuarios, tal como lo señala la denuncias por delitos informáticos registradas por Fiscalías Penales Comunes y Fiscalías Mixtas en el periodo 2020, en Lima con un total de 1116 denuncias y en el año 2019 con un total de 3713 denuncias, en Lima Norte con 220 denuncias, en Arequipa con 115, en la Libertad con 232 denuncias, Lambayeque 124 denuncias, en Callao con 101 denuncias, Cusco con 81 denuncias, Lima Sur con 119, Huánuco 36 denuncias, haciendo denotar el número elevado de denuncias.

Es por ello, que los doctores Rodríguez, Ramos y Amaya (2020) mencionan que las modalidades más frecuentes para la comisión de delitos de fraude informático son el Phishing, Smishing y Vishing. Estas se computan de la siguiente manera: para empezar el Phishing es un tipo de engaño creado por los hackers con fines delictivos para así obtener información confidencial como claves, tarjetas de crédito. Generalmente usan el

engaño para la comisión de estos actos delictivos, aprovechando la ignorancia del usuario para ingresar a páginas que no son auténticas para proporcionar sus datos. También se consolidan usando correos electrónicos de manera masiva para aparentar ser de entidades bancarias para obtener información al momento de introducirlos en la página falsa incluida en dicha comunicación de forma fraudulenta. Es una de las modalidades más usadas por los agentes activos y es la más común, ya que se basa en ingeniería social, el cual reemplaza la dirección del IP⁶ de los servidores para enviar un correo electrónico para poder dirigirlos a una página falsa con la intención de obtener información confidencial con un fin económico.

De modo que, una de los análisis que se pueden observar es la existencia de artículos generales en cuanto a la redacción de delitos informáticos como es la Ley de Delitos Informáticos n.º 30096, Art 8 Fraude informático⁷ no contemplan la realidad social de nuestro país, además de no contar con un texto normativo que definan de manera específica los tipos penales que se comenten con mayor frecuencia en la red. Con esto pudimos observar la falta de cultura informática, que es un factor muy importante para afrontar la ola de criminalidad informática. Es por ello que en cuanto al número de denuncias proporcionado por el Ministerio público por delitos informáticos durante el 2013 y 2020 según su estado procesal, existen 12,608 denuncias archivadas, 8,842 en proceso y 108 denuncias que terminaron en sentencia. A modo de conclusión, es imprescindible mencionar la carencia de información acerca de los límites de los delitos informáticos, el cual nos permite conocer el manejo de determinadas situaciones, asimismo proporcionar seguridad tecnológica al usuario al momento de manejar herramientas tecnológicas definir la normativa desde la realidad social de nuestro país.

OE1: Identificar cuáles son los elementos que deben ser considerados a fin de tipificar las conductas delictivas del *phishing*, *smishing* y *vishing*

HG1: Los elementos relevantes de carácter penal que deben ser tomadas en cuenta para las estructuraciones de los tipos penales del *phishing* son utilización de

⁶ IP: Es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red de un dispositivo que utilice el protocolo o que corresponde al nivel de red

⁷ Artículo 8. Fraude informático

El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos 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.

correos electrónicos en la que se incorpora medios digitales fraudulentos con fines de obtener información de terceros; por su parte el *smishing*, consideramos que tener contener la utilización de mensajes de texto en que la se incorpora medios digitales con fines defraudatorios; y con respeto al *vishing*, se debe considera los actos referidos a la utilización de llamadas telefónicas robotizadas y/o personales con fines defraudatorios.

Sobre los elementos que deben ser considerados para tipificar las conductas delictivas del *phishing*, *smishing* y *vishing*

Los elementos que deben ser considerados para tipificar las conductas delictivas mencionadas desde la dogmática jurídico penal con relación a los delitos informáticos se deben analizar desde un punto de vista normativo para la construcción de los tipos penales y así determinar que conducta se pretende imputar. Además de la transferencia no consentida o alterar la información que se encuentra en una base de datos, debemos tener en consideración que hoy en día existe una mayor facilidad de cometer delitos informáticos a través del internet y las múltiples capacidades de los usuarios para manejar un ordenador; es por ello que los delitos informáticos no pueden ser tratados de manera común, como pasa con los delitos tradicionales.

Por ello, los doctores Rodríguez, Ramos y Amaya (2020) sostienen que, partiendo de las conductas del *phishing*, *smishing* y *vishing*, son propias del ciber fraude; y aunque el fraude informático como tal está penalizado en la Ley de delitos informáticos en el Perú Ley 30086 y su modificatoria con la Ley 30171 como elementos objetivos del Phishing, Smishing y Vishing y el sujeto activo: el que (cualquier persona), y como verbo rector: remisión o envío de correo electrónico de manera unitaria o masiva además del envío de mensajes de texto a través de las TIC, realización de llamadas telefónicas, con la finalidad de obtención de datos personales que permitan acceder a sus cuentas. Asimismo, menciona que en la tipificación de dichas conductas lo primero es que proviene de una conducta fraudulenta; es decir, el que engaña al usuario para así obtener datos confidenciales. Segundo, que se basa en el dominio informático que posee el agente activo para la manipulación de los datos. Y, por último, debemos tener en consideración que la finalidad del autor del delito es obtener algún beneficio económico o personal.

Por consiguiente, el Derecho penal tiene como principio fundamental determinar cuál es el hecho penalmente relevante, y a quien se debe atribuir el ilícito penal. Es más, cuando

estas se realicen por medio de facultades intelectuales, como resultado es necesario determina el hecho antijurídico y con ello la imputación objetiva de la conducta típica, y la necesidad de la existencia de un resultado que constituye la realización de un riesgo jurídicamente relevante. Por ende, es necesario mencionar el principio de causalidad, el nexo de la acción y el resultado, para así atribuir al resultado a una determinada conducta para la imputación objetiva.

Sobre los elementos relevantes de carácter penal que deben ser tomadas en cuenta para las estructuraciones de los tipos penales del *phishing*, *smishing* y *vishing*

Los elementos objetivos del tipo para estructurar los ilícitos penales del *phishing*, *smishing* y *vishing* deben reunir todos los elementos correspondientes para que se acredite la tipicidad. Es por ello que primero debemos analizar el tipo penal, el cual sirve de instrumento legal para determinar y describir aquellas acciones que son penalmente relevantes para el derecho.

Ahora bien, las modalidades del *phishing*, *smishing* y *vishing* son las modalidades de estafa más común cometida en la red mediante el cual se usa la manipulación informática para la defraudación con el objetivo principal de obtener un beneficio y así causar un perjuicio patrimonial, definiéndolos como delitos de peligro y delitos consumados.

Segundo, es importante determinar el sujeto pasivo y activo de las modalidades del *phishing*, *smishing* y *vishing*. Para empezar, el sujeto activo es cualquier persona que tenga conocimientos básicos en informática que accede al sistema ilegítimamente o un tercero no autorizado. En cuanto al sujeto pasivo, este puede ser cualquier persona que se le haya vulnerado un bien jurídico.

Con respecto a la imputación subjetiva, para el tratamiento de los delitos informáticos el sujeto activo actúa de manera dolosa; en otras palabras, realiza la acción delictiva con pleno conocimiento y con intención. Por otro lado, para este tipo de delito no cabría la comisión culposa. Es necesario recalcar que para este tipo de delitos no podrían ser llevados a cabo por error, ya que dichas acciones requieren de un conocimiento básico. En conclusión, el sujeto activo tiene pleno conocimiento que su accionar constituye una acción contraria al derecho. Esto quiere decir para la comisión de los delitos informáticos en sus modalidades del *phishing*, *smishing* y *vishing*, el elemento subjetivo del injusto penal es definir cuál es el resultado de la acción; en otras palabras, el ánimo de lucro.

Con relación a esto, Roxin (1997) nos menciona que se cumple con el tipo objetivo cuando el comportamiento del sujeto activo haya creado un riesgo no permitido, cuando el riesgo haya producido un resultado concreto, y cuando el resultado se encuentre dentro de los alcances del tipo.

Una de los conflictos que nace a la hora de definir el tipo penal de los delitos informáticos y la facilidad que hoy se tiene para cometer delitos a través de medios informáticos. En ese sentido solamente basta con tener la capacidad de un usuario para manejar el sistema informático, ya es que las reglas que se aplican a delitos tradicionales se distorsionan en un espacio virtual. La doctrina menciona que los delitos de peligro abstracto para que sean aplicadas se toman en consideración la peligrosidad de la acción típica y la probabilidad de la lesión del bien jurídico

Consecuentemente, cabe mencionar que para la construcción del tipo penal es necesario el perjuicio de la acción típica; es decir, que como consecuencia de los actos cometidos por el sujeto activo cause un perjuicio económico al sujeto pasivo.

Tabla 8

Clasificación de delito

	Phishing	Smishing	Vishing
Por su gravedad	Bipartito	Bipartito	Bipartito
Por su acción	Acción	Acción	Acción
Por la ejecución	Instantáneo	Instantáneo	Instantáneo
Por las consecuencias de la acción	Formal: Mera actividad	Formal: Mera actividad	Formal: Mera actividad
Por la calidad del sujeto	Impropio: Cualquier persona	Impropio: Cualquier persona	Impropio: Cualquier persona
Por la calidad procesal	Acción pública	Acción pública	Acción pública
Por el elemento subjetivo	Doloso	Doloso	Doloso
Por el número de personas	Individuales o Colectivos	Individuales o Colectivos	Individuales o Colectivos
Por el bien jurídico vulnerado	Pluralidad Seguridad informática	Pluralidad Seguridad informática	Pluralidad Seguridad informática

Por su naturaleza intrínseca	Común vulnera a cualquier persona y social al sistema seguridad informático	Común vulnera a cualquier persona y social al sistema seguridad informático	Común vulnera a cualquier persona y social al sistema seguridad informático
Por el daño causado	Peligro: a que basta que surja un riesgo general, común, genérico (peligro abstracto) o, en todo caso, preciso, determinado, específico (peligro concreto)	Peligro: a que basta que surja un riesgo general, común, genérico (peligro abstracto) o, en todo caso, preciso, determinado, específico (peligro concreto)	Peligro: a que basta que surja un riesgo general, común, genérico (peligro abstracto) o, en todo caso, preciso, determinado, específico (peligro concreto)

Fuente: Elaboración propia a partir de los datos obtenidos por Lp pasión por el derecho <https://lpderecho.pe/cuales-las-trece-clasificaciones-del-delito/>

OE2 Determinar la naturaleza jurídica que debe adoptar la tipificación de las conductas delictivas del *phishing*, *smishing* y *vishing*

HG2 Los delitos que contemplen las conductas delictivas del *phishing*, *smishing* y *vishing* deben ser de naturaleza de delitos de mera actividad o delitos de peligro.

Sobre la naturaleza jurídica que debe adoptar la tipificación de las conductas delictivas del *phishing*, *smishing* y *vishing*

Con respecto al delito de resultado de las conductas del *Phishing*, *Smishing* y *Vishing*, según la Dra. Rodríguez (2020), considera que tienen que ser delitos de resultado, debido a que debe concretarse la acción como un efecto del comportamiento humano. Para esto, se debe entender que los delitos de resultado deben estar conectados a la acción; es decir, para que se concrete el delito de fraude informático este debe causar un resultado, es decir, una afectación del bien jurídico protegido por el Derecho. Este debe ser exteriorizado en un determinado espacio geográfico. Por otra parte, el resultado es la plasmación del injusto; es decir, la arbitrariedad de la punibilidad de la violación objetiva y subjetiva.

La valoración que hace la doctora con respecto a que se debe considerar que las modalidades del *phishing*, *smishing* y *vishing* sean delitos de resultado es también válida, por el simple hecho de la complejidad del tratamiento que se les da a los delitos informáticos, habiendo puesto al descubierto las carencias no solo legislativas si no también la tecnológicas. Esto complica aún más para los fiscales la persecución del delito

o si este ha cumplido con todos los elementos para imputar el delito. Es decir, la ley castiga el daño producido, aquel que deliberadamente e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos. En líneas generales, estaríamos hablando de un delito de resultado. Pero, ¿qué pasa cuando la persona no realiza un daño, pero si el espionaje de información confidencial? Muchos autores señalan a estas modalidades con el denominado nombre del ciberterrorismo, como un ataque premeditado motivado a causar posteriormente un daño a la información, programas, sistemas o datos. Para validar esta hipótesis tenemos que tener en cuenta que muchas empresas, negocios ya no operan con sistemas rudimentarios, y la perpetuación de esta información puede generar pérdidas económicas de manera masivas tales como la propagación de virus informáticos, el acoso mediante correos electrónicos de manera masiva, llamadas con fines fraudulento.

Respecto al delito de Peligro (concreto y abstracto)

Para este punto, según el decreto supremo, del Acuerdo Plenario 6-2006/CJ-116, siguiendo la definición de Enrique Bacigalupo, hace referencia a que para los delitos de peligro no es necesario que la conducta del agente ocasione un daño económico; sino que, la tipificación del objeto jurídicamente protegido se haya puesto en peligro, ya que lo que la norma pretende es evitar la consumación del acto delictivo. Es decir, con la intención de maniobrar la información valiéndose de habilidades tecnológicas la perpetue el sistema informático para obtener un provecho, ya se estaría computando el peligro.

Los delitos de peligro concreto hacen referencia a la probabilidad de la lesión del bien jurídico protegido a la cantidad de circunstancias para afirmar la existencia de un peligro. Esta se define según la cantidad de factores que pueden llevar a cabo la producción de un daño cercano, y la necesidad que un bien jurídico estén puesto en peligro. En esa misma línea, muchos autores señalan que es necesaria la causalidad concreta; es decir, si se verifica la falta de condiciones concretas estaríamos hablando de la falta de daño, de modo concreto, la falta de daño señala la insistencia de peligro

En cuanto a la naturaleza jurídica que debe adoptar la tipificación de las conductas delictivas, la doctrina explica que los delitos de peligro abstracto son aquellos delitos donde la consecuencia jurídica se debe tomar como consideración la peligrosidad de la acción típica y la posibilidad de la existencia de una lesión del bien jurídico. Es decir, basta el riesgo para la imputación típica. El tipo penal se consuma con la mera realización del comportamiento; en tal sentido, no es necesario que este afecte un bien jurídico de

carácter personal, de modo que las modalidades *phishing*, *smishing* y *vishing* podrían ser definidas como delitos de peligro puesto que, para la comisión de estos delitos no cabría la necesidad de una consumación del accionar, ya que deliberadamente estas modalidades son cometidas sabiendo el perjuicio que va a ocasionar. Es notable mencionar que solo aquel que tenga conocimientos básicos en ingeniería social puede perpetuar los ordenadores para incurrir en error al sujeto activo o tenga pleno conocimientos de los puntos para perpetuar un programa.

Sobre la contemplación de las conductas delictivas del *phishing*, *smishing* y *vishing* desde la perspectiva de los delitos de peligro en su aspecto de tipo base.

Como ya mencionamos con anterioridad, las conductas delictivas del *phishing*, *smishing* y *vishing* deben ser delitos de peligro abstracto debido a la estructura del delito en cuanto a la perturbación de los sistemas informáticos. Por otro lado, es suficiente la imputación del comportamiento. Los doctores Ramos y Amaya (2020) aseveran que para la comisión de los delitos informáticos no encaja en la comisión culposa, puesto que el sujeto activo actúa de manera dolosa; ya que conoce y quiere realizar la acción ilícita, puesto que para realizar la manipulación informática es necesario tener un conocimiento básico tecnológico. Ello implica la intención del sujeto activo, ya que siguiendo un orden lógico, para realizar la modificación, alteración de datos y programas, estas no pueden ser cometidas por error, ya que de ahí surge un aprovechamiento económico y que la naturaleza jurídica que se debe optar para la tipificación de estas modalidades en el ordenamiento jurídico es de peligro por el perfeccionamiento de la realización de la acción del sujeto activo; de modo que, para la comisión del acto, es necesario que el agente activo primero tenga conocimientos básicos en ingeniería social para realización de la defraudación

Sobre la contemplación de las conductas delictivas del *phishing*, *smishing* y *vishing* desde la perspectiva de los delitos de resultado en su aspecto de tipo agravado.

Ahora bien, habiendo definido que la tipificación de los delitos del *phishing*, *smishing* y *vishing* como delitos de peligro abstracto en primera instancia, ya que lo que busca es la protección de la acción, a su vez estas ameritan que su tratamiento se configure como delitos de resultado cuando se produzcan la consumación del tipo agravado del accionar delictivo

Cuando hablamos de delitos de resultado, se puede definir que se exige un resultado separado del espacio y tiempo de la acción como los delitos de homicidio. Esto a su vez

se diferencia con los delitos de mera actividad; es necesario que se consuma la realización de la acción del delito es imprescindible diferenciar los tipos penales, puestos que se encuentran fundamentados en la imputación objetiva. Es decir, la consumación del delito de mera conducta se crea bajo la premisa del riesgo prohibido mediante el cual la presente tesis pretende tipificar la acción delictiva del *phishing*, *smishing* y *vishing* y como agravante la consumación del acto que produzca el daño, sobre ella la existencia de una imputación objetiva de resultado.

No obstante, también es importante hablar de la clasificación que se hace con respecto a los delitos de lesión y de peligro abstracto; el primero se clasifica como delitos de resultado; es decir, que lesionen a un bien jurídico protegido, mientras que los delitos de peligro amenazan el objeto del bien jurídico protegido. Ahora bien, estaríamos hablando de delitos subsidiarios, ya que lo que se pretende es que, si bien es cierto las modalidades se configuren como delitos de peligro abstracto por cuanto, a su complejidad de identificar al agravado, esta se subsume cuando se produzca la consumación del accionar es decir hablaríamos de delitos de resultado. Por otro lado, un ejemplo claro es delito de Robo tipificado en el artículo 188 al 189 del Código Penal que se configura como delitos de resultado, pero este logra agravarse cuando el agente activo pertenezca a una organización criminal que se encuentra tipificado en el artículo 317° del Código Penal peruano cuyo bien jurídico es la tranquilidad pública “delitos de peligro abstracto”, ahí los delitos tendrían una naturaleza de subsidiaria.

4.1.3 Implicancias

En cuanto a las implicancias, como base de los objetivos de la investigación tomadas para su desarrollo, esta tesis se realizó bajo tres premisas: la implicancia práctica, teórica y metodológica, mediante el cual nos permitirá justificar la importancia de nuestra investigación ayudando así a la comunidad jurídica para la tipificación de las modalidades *phishing*, *smishing* y *vishing* en nuestro sistema penal y proporcionar seguridad jurídica a la población.

4.1.3.1 Implicancia practica

En referencia a la implicancia práctica, este trabajo contribuirá al Sistema de Administración de Justicia y sus operadores a resolver problemas sociales de manera efectiva. Primero porque la tipificación de las modalidades delictivas como el *phishing*, *smishing* y *vishing* servirá para que los agentes de justicia puedan realizar una debida persecución del delito y sancionarlas con la finalidad de crear seguridad informática y

romper con la incertidumbre jurídica que aqueja a los usuarios al momento de utilizar los TIC. Esta propuesta tiene un respaldo doctrinario, tomando en consideración la existencia de la Ley de Delitos Informáticos n.º 30096 y su modificatoria para combatir la lucha contra la delincuencia, estos no resultarían efectivos puesto que en la redacción sanciona los medios mediante el cual se comisiona el delito, mas no regula la conducta de la norma penal adjetiva pues cuentan con el respaldo de la doctrina, el análisis documental y las entrevistas obtenidas.

Posteriormente, la implicancia mencionada anteriormente es indispensable para mejorar los problemas que existen en nuestro sistema jurídico con respecto al tratamiento de las denuncias por delitos informáticos y poder encajar el tipo penal en nuestro sistema normativo, esto también beneficiara para delimitar mejor las conductas delictivas.

4.1.3.2 Implicancia teórica

Con respecto a la implicancia teórica, se puede inferir que los resultados obtenidos servirán para incrementar la información en materia de la ciberdelincuencia y apoyara a realizar más propuestas para mejorar el marco normativo con respecto a los delitos informáticos sobre el perjuicio de causa a la sociedad las formas delictivas que merecen ser tipificadas por su incurrancia en nuestro país. Además, podremos mejorar muchas más deficiencias como darle mayor publicidad a la sociedad sobre estas modalidades para evitar así ser víctimas de delitos informáticos, mejor capacitación las los agentes de justicia para la imputación del delito, la obtención, custodia y preservación de la prueba digital, propuestas de diligencias pertinentes para esclarecer los hechos y a los presuntos responsables, y, sobre todo, darle a los usuarios seguridad al momento de usar los TIC.

En tal sentido, también se dejó al descubierto que los Jueces y Fiscales no están preparados para investigar y juzgar las denuncias por delitos informáticos, ni tampoco cuentan con un texto normativo que encaje la conducta en nuestro Sistema Penal; y la falta de una debida especialización, así como también la falta de herramientas tecnológicas, logística a nivel nacional, de tal manera hacen deficiente su labor. Con ello, esta investigación propone realizar un texto normativo que ayude al Sistema Penal a sancionar la conducta del *phishing*, *smishing* y *vishing*.

4.1.3.3 Implicancia metodológica

En lo que corresponde a las implicancias metodológicas, se estableció la elaboración de tablas de Excel que permitieron la delimitación de los documentos por título, autor, fecha el cual nos permitió delimitar el periodo de nuestra investigación, además que nos

permitió realizar un análisis documental más ordenado para un óptimo entendimiento y así eliminar los posibles documentos que no eran útiles para nuestra investigación.

4.2 Conclusión

Casi para terminar en esta parte del presente estudio, se realiza la interpretación general de la investigación, y el análisis de los datos proporcionados por las entrevistas y análisis documentales; todos ellos vinculados a los problemas y objetivos, con la finalidad de dar respuesta a la hipótesis de la investigación.

Como primera conclusión, debemos mencionar que las modalidades del *phishing*, *smishing* y *vishing* aún no se encuentran reguladas en nuestra legislación, a pesar de ser las formas más comunes de defraudación usada para engañar a los usuarios que nace a partir de la globalización. Por el contrario, la ola de ciberdelincuencia tuvo accenso por la falta de prevención y publicidad tanto del estado, como el de las entidades bancarias, al no advertir a los usuarios a que no deben brindar información confidencial vía online.

Como segunda conclusión, como elementos objetivos para su tipificación el *phishing*, *smishing* y *vishing* y como elementos subjetivos la existencia de del dolo la intención para cometer el acto delictivo y el agraviado como tipo base el estado Ministerio del Interior, procuraduría del Sector interior, consecuentemente tipo agravado el usuario como agraviado directo.

Como tercera conclusión, la naturaleza jurídica que deben adoptar las modalidades del *phishing*, *smishing* y *vishing* como primera instancia se concebirían como delitos de peligro abstracto cuyo bien jurídico a proteger sería la seguridad informática, y segunda instancia cuando estos delitos logren agravarse la naturaleza jurídica cambiaría a delitos de resultado cuya finalidad es proteger al usuario.

Como cuarta conclusión, la ola indiscriminada de la ciberdelincuencia no solo se computa con el robo de la información confidencial, sino que además se está volviendo un negocio en la red, donde muchos sujetos compran malware “programa malicioso “para robar información.

Como quinta conclusión, se podría decir que nuestro actual sistema de administración de Justicia el Ministerio Público, Poder Judicial y la Policía Nacional del Perú aun poseen deficiencias legislativas para procesar la comisión de delitos informáticos, a partir de carencia de infraestructura y logística.

Como sexta conclusión, de los resultados podemos advertir que el *phishing*, *smishing* y *vishing* son modalidades que se realizan con fines lucrativos incluso estos se pueden externalizar, creando incertidumbre social, de tal forma que a pesar de ocasionar daños este aún no se encuentra tipificada en nuestra legislación.

4.3 Recomendación

Para esta parte se realizaron las siguientes recomendaciones cuyo objetivo primordial es que sirva de utilidad tanto para nuestros legisladores y usuarios, para así fortalecer nuestro Sistema de Administración de Justicia y poder generar seguridad informática para que los delitos informáticos no queden impunes en nuestra sociedad.

Como primera recomendación, es necesario que nuestros legisladores sepan diferenciar las modalidades del *phishing*, *smishing* y *vishing* como acciones de defraudación donde el agente activo induce en error al agente pasivo; este sin ánimo de perjudicarse a sí mismo para cometer el acto ilícito. Por lo tanto, no pueden ser tratados de manera tradicional.

Como segunda recomendación, establecer una sanción idónea para estos ilícitos penales del *phishing*, *smishing* y *vishing* como modalidades de peligro abstracto y establecer como agravante la consumación de las modalidades, ya que la aplicación de esta pena podrá reducir de manera efectiva la ciberdelincuencia. Por otra parte, es necesario tener en cuenta que el perpetuador necesita tener conocimientos básicos en ingeniería social, lo que involucra la existencia del dolo.

Como tercera recomendación, es necesario que los legisladores sepan diferenciar qué delitos ameritan su tipificación, ya que puede haber acciones que involucren medios tecnológicos, pero no necesariamente necesiten una tipificación en la Ley de Delitos Informáticos n.º 30096. Por otra parte, es indispensable que nuestros legisladores se encuentren actualizados y con ello nuestro ordenamiento jurídico. Ante una sociedad cambiante tecnológicamente, se incurre en la necesidad de adquirir nuevas formas de protección, regulando el marco normativo de acuerdo a nuestra realidad social.

TIPIFICACION DEL CÓDIGO PENAL PARA SANCIONAR EL DELITO DEL PHISHING, SMISHING Y VISHING

Características de la propuesta:

Se propone agregar un artículo que deba tipificar y sancionar el delito de *phishing*, *smishing* y *vishing*, ya que es necesario considerar que la sociedad sufre de una dinámica

evolutiva constante; es decir, no somos ajenos a la globalización. Es necesario recordar que el comportamiento del individuo también es cambiante, incluidos las ciencias y tecnologías; es por ello la necesidad de una actualización al Código Penal y la tipificación y sanción de estas nuevas modalidades de comisión de delitos que han sido creados por la nueva era digital que sufre el mundo. Una de las características de la ley es que este siempre debe estar acorde de la realidad social evitando así la impunidad e incertidumbre social.

Incidencia de la propuesta en la solución del problema:

Con la tipificación de las modalidades del *phishing*, *smishing* y *vishing* los administradores de justicia podrán juzgar los delitos mencionados con base a la normativa penal y encajar la conducta en el tipo penal protegiendo así bienes jurídicos supraindividuales y, sobre todo, que estos delitos no quedaran en la impunidad frente a una creciente ola de criminalidad informática que se han generado en el país. No obstante, debemos tener claro una de las problemáticas es que estos no han podido ser sancionados por la falta de existencia de una ley que los tipifique y reprima y por último este proyecto deberá contar con previa aprobación y posteriormente su publicación.

Exposición detallada de la propuesta:

- Primero, se debe realizar la tipificación y sanción en el Código Penal ya que no cubre con las necesidades sociales en nuestro país por el incremento de delitos informáticos
- Segundo. por la falta de capacitación e imputación de las modalidades mencionadas por parte de los operadores de justicia (Fiscalías, Juzgados y Policía) con respecto a la investigación preliminar y la recolección de las pruebas.
- Y tercero. la necesidad de actualizar el ordenamiento jurídico y darle un enfoque con respecto a nuestra realidad social en el que vive el país con respecto a la ciberdelincuencia.

CAPÍTULO V. REFORMATORIA AL CÓDIGO PENAL QUE TIPIFICA EL DELITO DE PHISHING, SMISHING Y VISHING

a) Artículo enumerado

Elementos objetivos del *phishing*, *smishing* y *vishing*

Sujeto activo: El que (cualquier persona)

Verbo rector: Remisión o envío de correo electrónico de manera unitaria o masiva, él envió de mensajes de texto a través de los medios tecnológicos, y/o realización de llamadas telefónicas con la finalidad de defraudar patrimonialmente a una persona natural y/o jurídica mediante la obtención de información confidencial.

- El quien mediante el uso de ingeniería social, remite o envía correos electrónicos de manera unitaria o masiva, envía mensajes de texto a través de los medios tecnológicos, realiza llamadas telefónicas instantáneas o robotizadas con la finalidad de defraudar patrimonialmente a una persona natural y/o jurídica mediante la obtención de información confidencial, como puede ser contraseñas, datos de tarjetas bancarias, claves de acceso a la banca virtual, con el ánimo de apropiarse de un bien ajeno, en perjuicio de esta o de un tercero, será sancionado con pena privativa de libertad no menor de cuatro y no mayor de seis años.
- La pena será no menor de seis años ni mayor de ocho años cuando:
 - o El monto defraudado supere la remuneración mínima vital.
 - o La defraudación se produce sobre bonos de ayuda social otorgados por el Estado o cualquiera de los órganos de éste.
 - o Afecte al patrimonio del Estado destinado a fines asistenciales o programas de apoyo social.
 - o El agente actúe en calidad de miembro de una organización criminal

Agraviado: Tipo base el Estado (Ministerio del Interior, Procuraduría del Sector Interior⁸), tipos agravados el usuario (agraviado directo).

Elementos subjetivos: Dolo

⁸ Art. 5.2. 2) Producir, coordinar y centralizar la inteligencia estratégica y táctica, relacionada al orden interno, seguridad pública, seguridad ciudadana, crimen organizado y nuevas amenazas de carácter internacional que afecten el orden interno; así como realizar acciones de contrainteligencia en el marco del Sistema de Inteligencia Nacional.

b) Validación de la propuesta planteada

Esta propuesta está respaldada por los especialistas entrevistados, quienes consideran que es necesaria una pronta tipificación puesto que la tecnológica asume un rol fundamental en nuestra sociedad; considerando que no nos imaginamos que muchas actividades cotidianas ahora se manejen mediante los TIC. También, significara un aporte importante para la Administración de justicia dado que el phishing, *smishing* y *vishing* son modalidades de delito informático que han tenido mucho auge. Al no encontrarse tipificados en nuestra legislación, ocasionaría incertidumbre en la sociedad debido a una falta de protección.

c) Por qué es necesario sancionar el delito de phishing, smishing y vishing

Primero, porque es necesario que la sociedad se informe acerca de la prevención de los ilícitos penales del *phishing*, *smishing* y *vishing*; asimismo, conocer donde pueden realizar las denuncias correspondientes cuando hayan sido víctimas de estas modalidades.

Segundo, que es necesario que los usuarios desarrollen una cultura informática para que estén alertas de las diferentes modalidades de comisión de delitos informáticos y procuren utilizar los medios informáticos de una manera adecuada.

Tercero, desarrollar mecanismos de seguridad informática para proteger la información en sus distintos ámbitos, mejorar los mecanismos para la imputación del delito, sobre todo de la recaudación de la prueba de los delitos informáticos.

Cuarto, el Perú ha optado ser parte del convenio de Budapest para mejorar los mecanismos con respecto a la persecución de los delitos informáticos. No obstante, estos siguen siendo deficientes, ya que es necesario tener en cuenta que la tecnología es evolutiva y las formas de cometer delitos están en constante cambio.

Y, por último, la tesis busca prevenir y sancionar conductas ilícitas que afectan a los datos informáticos mediante la utilización de los TIC cuya finalidad es la lucha contra la ciberdelincuencia.

REFERENCIAS

- Arteaga, G. (2020). *¿Qué es el análisis de datos? Métodos, técnicas y herramientas*. Recuperado de <https://www.testsiteforme.com/tecnica-de-procesamiento-y-analisis-de-datos/>
- Arias Gonzáles, J. (2020). *Técnicas e instrumentos de investigación científica*. Recuperado de <http://bit.ly/2YFtw2Y>
- Arias Gonzáles, J. (2020). *Técnicas e instrumentos de investigación científica*. Recuperado de <http://bit.ly/2YFtw2Y>
- Avalos Rivera, Z. (2020). *Informe de análisis n°04 ciberdelincuencia: pautas para una investigación fiscal especializada*. Recuperado de <https://cdn.www.gob.pe/uploads/document/file/1669400/CIBERDELINCUCIA>
- Acurio del Pino, S. (2018). *Delitos informáticos generalidades*. Recuperado de https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf
- Altamirano Almanza, F (2010). *Teoría del delito*. Recuperado de <https://derecho.usmp.edu.pe/instituto/novedades/libro-teoria-del-delito-oscar-pena.pdf>
- Barboza Camelo, M. (2018). *Análisis del delito de fraude electrónico: Modalidad tarjeta de crédito*. Recuperado de https://repository.ucc.edu.co/bitstream/20.500.12494/8381/1/2019_analisis_delito_fraude.pdf
- Bank, A. (2020). *Ciberseguridad riesgos y avances y el camino a seguir América Latina y el Caribe*. Recuperado de <https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf>
- Ballina, G. (2008). *La evolución de internet como medio de comunicación masivo*. Recuperado de http://biblioteca.usac.edu.gt/tesis/16/16_0599.pdf
- Bajes Santacana, J. (2020). *La tentativa en los delitos de peligro abstracto*. Recuperado de <https://www.tesisenred.net/handle/10803/663023>

Coello Mazuelos, J. (2020). *El derecho de crédito como objeto de protección penal.*

Recuperado de

<file:///C:/Users/usuario/Downloads/14361-Texto%20del%20art%C3%ADculo-57143-1-10-20151117.pdf>

Curio del Pino, S. (2016), “*Delitos informático Generales*”.

Recuperado

de

https://www.oas.org/juridico/spanish/cyb_ecu_delitos_inform.pdf

Chocobar Reyes. M. (2019). *Transformación digital en marcha.* En el diario oficial el peruano. Recuperado de

<https://elperuano.pe/noticia/87889-transformacion-digital-en-marcha>

Diagnostico situacional sobre la Ciberdelincuencia en el Perú estadística DIVINDAT-DIRINCRI PNP. (2020).

Recuperado <https://cdn.www.gob.pe/com>

Espinoza Coila, M. (2017). *Derecho penal informático: deslegitimación del poder punitivo en la sociedad de control.* Recuperado de

<http://repositorio.unap.edu.pe/handle/UNAP/6309>

Flores, M. (2018). *Tecnología y violencia en Perú.* En *Hiper derecho.* Recuperado de <https://bit.ly/3oJbmbf>

Fuentes Garrido, K. (2021). *Modificación de la ley 30096 para incorporar los delitos de phishing, pharming y carding como delitos penalizables con prisión, para reducir la ciberdelincuencia, lima 2019.* Recuperado de

<https://repositorio.uss.edu.pe/handle/20.500.12802/8345>

García, R. (2021). *Definición del término Smishing.* Recuperado de

<https://www.bbva.com/es/phishing-y-smishing-que-son-y-como-evitarlos/>

Informe N°4 del Ministerio Público y la oficina de análisis de estratégico contra la criminalidad. (2021). Recuperado de

<file:///C:/Users/usuario/Documents/%20QUE%20USO/Informe%20N%C2%B04%20Unidad%20Fiscal%20Ciberdelincuencia.pdf>

Informe de la policía nacional del Perú dirección de investigación criminal división de investigación de delitos de alta tecnología N°113. (2020)

- López, P. (2004). *Población y muestra y muestreo*. Recuperado de <http://www.scielo.org.bo/pdf/rpc/v09n08/v09n08a12.pdf>
- López, M. (2021). *Qué es el vishing: estafa a través de llamadas o mensajes de voz*. Recuperado de <https://www.welivesecurity.com/la-es/2021/05/03/que-es-vishing/>
- Los TIC, (2017). ¿Qué es un ciberdelito? Recuperado de <https://bit.ly/2MJ0oVR>
- Perú se adhiere a Convenio de Budapest sobre Ciberseguridad y Ayuda Judicial. (04 de febrero de 2019).
Recuperado de <https://bit.ly/3r5S80Q>
- LP Pasión por el Derecho (2020). *Delitos de peligro abstracto y concreto*. Recuperado de <https://lpderecho.pe/tag/delitos-de-peligro-abstracto/>
- LP Pasión por el Derecho (2020). *Tipos penales*. Recuperado de <https://lpderecho.pe/cuales-son-las-clases-de-tipos-penales-bien-explicado/>
- Maldonado Muñoz, G. (2018). *La investigación cualitativa*. Recuperado de <https://www.uaeh.edu.mx/scige/boletin/tlahuelilpan/n3/e2.html>
- Medina Napuri, L. (2018). *Técnicas e instrumentos de la Investigación*. Recuperado de <http://repositorio.autonoma.edu.pe/bitstream/AUTONOMA/857/1/Medina%20Napuri%2C%20Leyla%20Alexandra.pdf>
- Mejía Mejía, M. (2005). *Técnicas e instrumentos de investigación*. Recuperado de <http://online.aliat.edu.mx/adistancia/InvCuantitativa/LecturasU6/tecnicas.pdf>
- Navarro Camacho, M. (2016). *Epistemología, Ciencia y Educación Científica: premisas, cuestionamientos y reflexiones para pensar la cultura científica*. Recuperado de <https://www.scielo.sa.cr/pdf/aie/v17n3/1409-4703-aie-17-03-00774.pdf>
- Observatorio Peruano de Cibercriminalidad-Fraudes Virtuales, (2020). Recuperado de <https://cibercrimenperu.com/publicaciones>
- Proyecto de Ley 5630/ (2020). *Ley de seguridad informática y represión de los delitos informáticos*. Por la congresista Robertina Santillana Paredes
- Persman, G. (2014). *Métodos y recolección y análisis de datos*.
https://www.unicef-irc.org/publications/pdf/brief_10_data_collection_analysis_spa.pdf

Rodríguez García. (2020). *Una aproximación al delito de estafa en sus modalidades clásica e informática: De la estafa tradicional a las nuevas modalidades como el Phishing*. Recuperado de

[https://ruc.udc.es/dspace/bitstream/handle/2183/27015/Rodr%
c3%adaJos%c3%a9David_TFM_2020.pdf?sequence=2&isAllowed=y](https://ruc.udc.es/dspace/bitstream/handle/2183/27015/Rodr%c3%adguezGarc%c3%adaJos%c3%a9David_TFM_2020.pdf?sequence=2&isAllowed=y)

Romero Castro, M. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades*. Recuperado de

[https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-
inform%C3%A1tica.pdf](https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf)

Salazar, N. (2007). “*PHISHING: LA AUTOMATIZACIÓN DE LA INGENIERÍA SOCIAL*”. Recuperado de

[https://repository.eafit.edu.co/bitstream/handle/10784/2443/Salazar_Natalia_200
7.pdf;jsessionid=7BC6751D6F2D39763B97351CFBFC51EC?sequence=1](https://repository.eafit.edu.co/bitstream/handle/10784/2443/Salazar_Natalia_2007.pdf;jsessionid=7BC6751D6F2D39763B97351CFBFC51EC?sequence=1)

Schwartz, M. (2020). *Reporte ciberseguridad riesgos, avances y el camino a seguir en américa latina y el caribe*. Recuperado de

[https://publications.iadb.org/publications/spanish/document/Reporte-
Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-
y-el-Caribe.pdf](https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf)

Sánchez, C. (2018). *Bienes Jurídicos*. Recuperado de

[file:///C:/Users/usuario/Downloads/DialnetLesividadEnLosBienesJuridicosColec
tivosYDelitosDeP-5235020.pdf](file:///C:/Users/usuario/Downloads/DialnetLesividadEnLosBienesJuridicosColec%20tivosYDelitosDeP-5235020.pdf)

Tomayo, M. (2002). *El proceso de la Investigación Científica*. Recuperado de

[http://evirtual.uaslp.mx/ENF/220/Biblioteca/Tamayo%20Tamayo-
El%20proceso%20de%20la%20investigaci%C3%B3n%20cient%C3%ADfica%20
02.pdf](http://evirtual.uaslp.mx/ENF/220/Biblioteca/Tamayo%20Tamayo-El%20proceso%20de%20la%20investigaci%C3%B3n%20cient%C3%ADfica%2002.pdf)

Vílchez Limay, R. (2020). *La ciberdelincuencia en el contexto de la pandemia del coronavirus. Una aproximación desde el marco convencional*. Recuperado de

[file:///C:/Users/usuario/Downloads/25688-Texto%20del%20art%C3%ADculo-
88341-1-10-20210209%20\(1\).pdf](file:///C:/Users/usuario/Downloads/25688-Texto%20del%20art%C3%ADculo-88341-1-10-20210209%20(1).pdf)

Vallejo, A. (2018). *Delitos de peligro abstracto*. Recuperado de

<https://www.tesisred.net/handle/10803/663023#page=1>

Zevallos Padro, O. (2020). *Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce?* Recuperado de <https://ius360.com/delitos-informaticos-cuales-son-los-principales-fraudes-informaticos-que-se-pueden-cometer-a-traves-del-e-commerce-oscar-zevallos-prado/>

ANEXOS

Anexo 1. Cuestionario de entrevista los abogados y fiscales especialistas.



“La Tipificación del Phishing, Smishing y Vishing en nuestro Sistema Penal Peruano para la lucha contra la Ciberdelincuencia, Lima 2020”.

Cuestionario para la entrevista

Título: “LA TIPIFICACIÓN DEL PHISHING, SMISHING Y VISHING EN NUESTRO SISTEMA PENAL PERUANO, PARA LA LUCHA CONTRA LA CIBERDELINCUENCIA EN LIMA, 2020”

Objetivo general: Justificar por qué las modalidades del Phishing, Smishing y Vishing deben ser incorporadas en el Sistema Penal, como delitos penalizados en el Perú.

NOMBRE Y APELLIDOS	Jose Lavin Morales	GENERO	F	M
INSTITUCION	Policia Nacional del Peru	NUMERO DE TELEFONO	982331181	
CORREO ELECTRONICO	Jose.lavin@pnp.gob.pe			
CARGO	Policia cargo administrativo			

1. ¿Considera que los delitos como el Phishing, Smishing y Vishing deben ser incorporados y penalizados en nuestro sistema de justicia?
2. En caso que su respuesta fuera afirmativa para penalizar los conductos del Phishing, Smishing y Vishing, ¿cuáles serian los elementos objetivos que deben ser considerados a fin de tipificar dichas conductas?
3. ¿Qué naturaleza jurídica debe adoptar la tipificación de las conductas delictivas del Phishing, Smishing y Vishing, de resultado o de peligro?
4. ¿El Perú ofrece programas de capacitación o de información en delincuencia cibernética a la policía, los procuradores, fiscales, agentes de la justicia y a la población en general?
5. ¿Afectaría a la seguridad informática las modalidades del Phishing, Smishing y Vishing en caso de tipificarse como conductas delictivas, o solamente a bienes jurídicos personales?
6. ¿Cuáles son las modalidades más frecuentes en el Perú, para la comisión del delito de fraude informático?
7. Desde la adhesión al Convenio de Budapest 2019 y la Ley N°30096, ¿El Perú ha podido minimizar los casos de Delitos informáticos?
8. ¿Existe hoy en día para los operadores de justicia alguna dificultad para la investigación y remediación de pruebas?
9. ¿Existe incremento anual de Delitos informáticos?
10. ¿Cuáles son delitos informáticos más recurrentes durante el periodo del 2020?

Anexo 2. Cuestionario de entrevista al efectivo policial

Cuestionario para la entrevista

Título: “LA TIPIFICACIÓN DEL PHISHING, SMISHING Y VISHING EN NUESTRO SISTEMA PENAL PERUANO, PARA LA LUCHA CONTRA LA CIBERDELINCUENCIA EN LIMA, 2020”

NOMBRES Y APELLIDOS	GENERO	F	M
INSTITUCION	NUMERO DE TELEFONO		
CORREO ELECTRONICO			
CARGO			

1. ¿Considera que la DIVINDAT cuenta con los recursos logísticos suficientes para atender las denuncias a nivel nacional?
2. ¿Cuál es el procedimiento para la atención de una denuncia interpuesta en provincia por la comisión de un presunto delito informático?
3. ¿A qué se debe el incremento anual de los delitos informáticos?
4. ¿Considera usted que el Fiscal actualmente se encuentra capacitado para investigar plenamente los delitos informáticos?
5. ¿Cuáles son los delitos informáticos más recurrentes en la DIVINDAT durante el 2020?
6. ¿Qué aspectos cree usted que se puedan potenciar en el Sistema de Justicia para la atención idónea de los casos de Ciberdelincuencia?

Anexo 3: Lista de entrevistados

ESPECIALISTA	RESUMEN DE HOJA DE VIDA	DATOS DEL ENTREVISTADO
MARISOL RODRÍGUEZ CHERO	Trabaja actualmente en el Ministerio Público-Fiscalía de la Nación, fiscal adjunta provincial titular de la fiscalía provincial especializada contra la criminalidad organizada de Piura	Marisolrodriguez022@hotmail.com
JIMMY PERCY RAMOS PICÓN	Trabaja actualmente en el Ministerio Publico de Huánuco, es Fiscal adjunto en la Primera fiscalía provincial de Huánuco	jimmi_235@hotmail.com
JOEL LEIVA MONTALVO	Sub oficial de tercera, actualmente se desempeña como efectivo policial de la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional del Perú.	Joel_Leiva@gmmail.com
LUIGHY AMAYA AGUERO	Abogado por la Universidad de Lima, Árbitro en Cámara de Comercio de Ica, Estudió en Universidad San Martín De Porres Facultad De Post Grado Derecho	Amaya_Luighy@gmail.com
FRANZ HENDRIK LOARDO OTAYZA	Abogado por la Universidad Unheval – Huánuco, trabajo como fiscal adjunto en amarilis, cuenta con una maestría en Ciencias Penales por la Unheval. Con estudios de investigación criminal.	Hendrik_Franz_condultor@gmail.com

Anexo 3. Solicitud de acceso a la información pública

The screenshot shows a Gmail interface with a search bar containing 'in:sent'. The left sidebar includes folders like 'Recibidos' (2,765), 'Destacados', 'Pospuestos', 'Enviados', 'Borradores' (27), 'Unwanted' (1), 'Más', 'Meet' (Nueva reunión, Unirse a una reunión), and 'Hangouts' (Mishell Alisson). The main email content is as follows:

Solicitud para fines académicos

Mishell Alisson Ventura Quijano <alisson25mishell@gmail.com> para dircima.ceopol, dircima.divprepu, dircima.dir
mar, 7 sept 13:51

Buenas tardes, mi nombre es Mishell Alisson Ventura Quijano soy alumna de la Universidad Privada del Norte, el motivo de mi mensaje es el siguiente soy bachiller de Derecho y Ciencias Políticas, estoy realizando mi tesis de titulación mi tema se trata sobre **"La Tipificación del Phishing, Smishing y Vishing en nuestro Sistema Penal Peruano"** teniendo conocimiento del arduo trabajo de la DIVINDAT para tratar esta clase de delitos quisiera solicitar encarecidamente una entrevista virtual según su disposición y horario, de un miembro de esta división, dicha entrevista es realizada con fines académicos, sin mas que decir espero su pronta respuesta y de antemano muchas gracias.

Datos de contacto

- Código de estudiante : N00158849
- Numero de DNI: 78459380
- numero de celular: 926695373

Buttons: Responder, Responder a todos, Reenviar

Anexo 4. Observatorio Peruano de Cibercriminalidad sobre Nuevas Tecnologías y Delitos Informáticos



Anexo 5: Proyecto de Ley 5630/2020 -Ley de seguridad informática y represión de los delitos informáticos por la congresista Robertina Santillana Paredes



Problema	Objetivos	Hipótesis	Variables	Dimensiones	Metodología
<p>Problema general</p> <p>¿Las modalidades delictivas del Phishing, Smishing y Vishing se encuentran recogidas en la legislación peruana?</p> <p>Problemas específicos</p> <p>¿Cuáles son los elementos que deben ser considerados a fin de tipificar las conductas delictivas del Phishing, Smishing y Vishing?</p> <p>¿Qué naturaleza jurídica debe adoptar la tipificación de las conductas delictivas del Phishing, Smishing y Vishing?</p>	<p>Objetivo general</p> <p>Justificar por qué los delitos del Phishing, Smishing y Vishing deben ser incorporados en el Sistema Penal como delitos penalizados en el Perú.</p> <p>Objetivos específicos</p> <p>Identificar cuáles son los elementos que deben ser considerados a fin de tipificar las conductas delictivas del Phishing, Smishing y Vishing</p> <p>Determinar la naturaleza jurídica que debe adoptar la tipificación de las conductas delictivas del Phishing, Smishing y Vishing</p>	<p>Hipótesis general</p> <p>Las modalidades delictivas del Phishing, Smishing y Vishing no se encuentran reguladas en la legislación peruana, en ese sentido, a la fecha existe cierta impunidad de estas conductas.</p> <p>Hipótesis específicas</p> <p>Los elementos relevantes de carácter penal que deben ser tomadas en cuenta para las estructuraciones de los tipos penales del Phishing son utilización de correos electrónicos en la que se incorpora medios digitales fraudulentos con fines de obtener información de terceros; por su parte el Smishing, consideramos que tener contener la utilización de mensajes de texto en que la se incorpora medios digitales con fines defraudatorios; y con respecto al Vishing, se debe considera los actos referidos a la utilización de llamadas telefónicas robotizadas y/o personales con fines defraudatorios.</p> <p>-Los delitos que contemplen las conductas delictivas del Phishing, Smishing y</p>	<p>Variable independiente</p> <p>Incorporar delitos como el Phishing, Smishing y Vishing.</p> <p>Variable dependiente</p> <p>Sistema Penal del Perú.</p>	<p>Administración de Justicia</p> <p>Es el aparato del Estado puesto al servicio de la administración de justicia, directa o indirectamente a través del Poder Judicial, el Ministerio Público y otras entidades públicas.</p> <p>Ley de Delitos Informáticos N°30096</p> <p>Tiene como objetivo prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos, la indemnidad y libertad sexuales, la intimidad y el secreto de las comunicaciones, el patrimonio y la fe pública.</p>	<p>Propósito: Básica</p> <p>Enfoque: Mixto (Cualitativo y Cuantitativo)</p> <p>Diseño: No experimental</p> <p>Alcance o nivel: Exploratorio</p> <p>Método: Sociológico</p> <p>Población:</p> <p>P1: Especialistas en la materia nacionales.</p> <p>P2: Base de datos de los casos seguidos en sede fiscal y judicial</p> <p>Muestra: Muestreo no probabilístico por conveniencia:</p> <p>M1: 2 fiscales especialidades en ciberdelincuencia.</p> <p>M2: 3 abogados especialistas nacionales.</p> <p>M3: 1 efectivo policial de la DIVINDAT.</p> <p>M4: Reporte fiscal con 15 548 casos desde el año 2015 hasta el 2020.</p>

		Vishing deben ser de naturaleza de delitos de mera actividad o delitos de peligro.			<p>M5: Reporte judicial con 440 sentencias condenatorias desde el año 2016 hasta el 2020.</p> <p>Técnica de recolección de datos: Entrevista no estructurada Análisis de documentos</p> <p>Instrumento de recolección de datos: Guía o cuestionario de entrevista (Enfoque cualitativo) Análisis documental (Enfoque cuantitativo)</p> <p>Método de análisis de datos: Tablas dinámicas y gráficos en Excel.</p>
--	--	--	--	--	---

Anexo 6: Matriz de consistencia