UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

PROGRAMA ACADÉMICO DE MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021

TESIS PARA OBTENER EL GRADO ACADÉMICO DE:

Maestra en Derecho Penal y Procesal penal

AUTORA:

Carrera Peña, Iveett del Rosario (ORCID: 0000-0003-4071-6241)

ASESOR:

Dr. Gallarday Morales, Santiago Aquiles (ORCID: 0000-0002-0452-5862)

LÍNEA DE INVESTIGACIÓN:

Derecho Procesal Penal

LIMA – PERÚ

2021

Dedicatoria

A mis amados padres Freddy y Silvia por sus enseñanzas, sacrificio y esfuerzo, sin ello no sería la persona que soy en la actualidad.

A mis adorados hijos Sebastián y Luciana por ser fuente de inspiración y motivación para poder superarme cada día más y luchar por un mejor futuro.

A mi querido Jean Franco por su comprensión, cariño y apoyo incondicional, por estar siempre a mi lado en los momentos más turbulentos.

Agradecimiento

Agradezco a Dios por brindarme una familia maravillosa, quienes siempre han creído en mí, y me dieron el mejor ejemplo de superación, humildad y sacrificio.

A mi asesor Santiago Aquiles Gallarday Morales por su apoyo y conocimientos que hicieron posible esta investigación.

Índice de contenidos

Carátula

Dedicatoria ii

Agradecimiento iii

Índice de contenidos iv

Índice de tablas v

Resumen vi

Abstract vii

I. INTRODUCCIÓN 1

II. MARCO TEÓRICO 4

III. METODOLOGÍA 14

3.1. Tipo y diseño de investigación 14

3.2. Categorías, subcategorías y matriz de categorización 14

3.3. Escenario de estudio 15

3.4. Participantes 15

3.5. Técnicas e instrumentos de recolección de datos 16

3.6. Procedimiento 17

3.7. Rigor científico 17

3.8. Método de análisis de la información 18

3.9. Aspectos éticos 18

IV. RESULTADOS Y DISCUSIÓN 19

V. CONCLUSIONES 28

VI. RECOMENDACIONES 33

REFERENCIAS 31

ANEXOS 36

Anexo 1 – Matriz de categorización

Anexo 2 – Matriz de triangulación

Anexo 3 – Guía de entrevista

Anexo 4 – Guia de entrevistas desarrolladas

Anexo 5 – Declaratoria de originalidad del autor

Anexo 6 – Autorizacion de publicacion en repositorio institucional

Índice de tablas

Tabla 1: Caracterización de participantes 16
Tabla 2: Propósito de técnicas e instrumentos 16

Resumen

La presente investigación ostenta como objetivo general, determinar las deficiencias en las investigaciones por delito de fraude informático en el distrito de Lima – 2021. Como objetivos específicos se buscó analizar como la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de lima.

Ello, con una aproximación doctrinal y legal al fenómeno detectado, en la categoría principal, las investigaciones por delitos de fraude informático; con sub-categorías, i) la deficiente investigación fiscal y ii) falta de conocimiento y dominio en delitos de fraude informático.

Se empleó un método no experimental, desde un enfoque cualitativo, tipo básico y diseño de investigación fenomenológico. Para la muestra se aplicó la entrevista a los diferentes expertos en la materia, como fiscal adjunto provincial, asistente en función fiscal y abogados defensores en el distrito fiscal de Lima. Como resultado se pudo determinar que las principales deficiencias es la falta de capacitación a las diversas modalidades informáticas que se presentan a la actualidad, perjudicando el curso y dirección de las investigaciones fiscales por estos ilícitos, la misma que además no cuenta con un respaldo normativo.

Palabras Claves: deficiencias en las investigaciones, delitos informáticos, delitos de fraude y fraude informático.

Abstract

The general objective of this investigation is to determine the deficiencies in the investigations for computer fraud crimes in the district of Lima - 2021. As specific objectives, it was sought to analyze how the deficient fiscal investigation harms the investigations for computer fraud crimes in the fiscal district from Lima.

This, with a doctrinal and legal approach to the phenomenon detected, in the main category, investigations for crimes of computer fraud; with sub-categories, i) deficient tax investigation and ii) lack of knowledge and mastery in computer fraud crimes.

A non-experimental method was used, from a qualitative approach, basic type and phenomenological research design. For the sample, the interview was applied to the different experts in the matter, such as provincial deputy prosecutor, assistant in prosecutorial function and defense lawyers in the fiscal district of Lima. As a result, it was determined that the main deficiencies are the lack of training in the various computer modalities that are currently presented, damaging the course and direction of tax investigations for these crimes, which also does not have regulatory support.

Keywords: deficiencies in investigations, computer crimes, fraud crimes and computer fraud.

I. Introducción

A lo largo de los últimos años la masificación del internet nos ha otorgado innumerables beneficios, tanto a la esfera académica y social, llegando a considerarse una herramienta vital irremplazable; sin embargo, también permitió la apertura de una ventana para conductas delictivas (ciberdelincuencia), pues como muchos avances, ha traído consecuencias negativas y deficiencias en su funcionamiento, durante el 2020 se ha podido advertir un sin número de casos registrados por delitos informáticos, los cuales han cobrado nuevas víctimas a causa de información contenida en diversos correos, publicidad y/o enlaces falsos que utilizan datos, para ocasionar una exposición y disposición en el patrimonio de muchos usuarios (Alansari, Zainab y Muhammad, 2019).

Ante lo expuesto resulta útil hacer mención a que este problema también se ve reflejado en el aspecto internacional, como por ejemplo en España, Devia (2017), expresa que, el 81.307% de los delitos en total son actos cometidos por delitos cibernéticos, debido que hasta el momento a pesar de las normas interpuestas se sigue presentando una estafa informática, es por ello que se requiere que el Estado mejore la norma informática de acuerdo a la realidad social, aplicando opiniones jurisprudenciales que toman en cuenta la nueva forma de criminalidad tecnológica, del mismo modo en México, Ochoa (2020) citando a Solís, expresa que la legislación de delitos informáticos de México va por buen camino, no obstante, anuncia que los problemas ya no se presentan bajo las mismas herramientas de un fraude información, sino aplican nuevas herramientas electrónicas como el SMiShing, ante ello se requiere capacitar a los ministerios públicos y jueces sobre los ciberataque (Nurse, 2018), así como implementar una policía cibernética que ayuden a mejorar la ciberseguridad, de igual manera sucede en Argentina, Roibón (2019), manifiesta que en el año 2018 se presentó el doble de incidentes de ciberseguridad en las empresas, en donde se detectó 159.000 datos que han sido cogidos por Ransomware, el cual es un programa que restringe el acceso de información empresarial, ante ello el autor menciona que para darle una solución al problema de los delitos informáticos no se requiere una

modificación normativa, ni una creación de nuevos delitos, sino que los operadores judiciales se encuentren preparados para perseguir nuevos hallazgos delictivos, bajo la misma línea en Chile, Mayer y Oliver (2020), determinan que hasta la fecha el desarrollo del comercio electrónico a incrementado nuevas modalidades de fraude informático como son el pharming, hacking, sabotaje informático y estafa cibernética, es por ello plantea tomar en consideración lo manifestado por el Convenio de Ciberdelincuencia del Consejo de Europa para tipificar el fraude información dentro del ordenamiento jurídico Chileno, tomando en cuenta la conducta de manipulación del agente, el perjuicio patrimonial y la presencia de ánimo de lucro, otro claro ejemplo de problema lo presenta Venezuela, ante ello Herrera (2020), cita a la ex fiscal Fernández, quien establece que durante la pandemia Covid-19 la ciberdelincuencia aumentado mucho más que años anteriores, esto se genera debido a que las personas desean obtener información que estén ligadas a la tecnología y comunicación, es por ello que como solución interpone la existencia de un Cuerpo de Investigaciones Científicas, Penales y Criminales (Cicpc), para evitar ciberataques, proporción de datos por correo y difusión de mensajes falsos, así mismo en Paraguay, Sequera y Samaniego (2018), pretende crear un programa de Policy Paper que permita controlar la confidencialidad, integridad y disponibilidad de los sistemas informáticos.

Como se ha podido apreciar este problema se desarrolla en diferentes Estados y Perú no es ajeno a ello, es por ello que Zevallos, (2020), hace mención que los delitos cibernéticos dentro del Estado peruano han aumentado por la problemática del Covid-19, donde se toma como relevancia jurídica la Ley N. ° 30096 y su modificatoria Ley N° 30171, sin embargo, el problema persiste cuando se incrementa el comercio electrónico a través de la compra y venta de productos, es por ello que el autor requiere que la Oficina Técnica del Ministerio Público incremente nuevas modalidades a fin de identificar a los ciberdelincuentes, singular opinión comparte Castillo (2020), el cual establece que a pesar de la Ley de Delitos Informáticos y la Unidad Policial Especializada, el Estado peruano en el año 2020 aun presento estadísticas en aumento sobre los casos de ciberdelito, pues hasta el momento no hay ninguna solución jurídica que recaigan sobre dichos problemas, es por ello que recomienda capacitar a los fiscales y jueces sobre los delitos informáticos, esto se ve reflejado en

los informes expuestos por el Ministerio Publico (2020), donde esta conducta ha generado un incremento considerable de 21,687 ingresos de denuncias por delitos informáticos ante las Fiscalías Penales Comunes Especializadas y Fiscalías Mixtas, conforme se aprecia en el reporte de la Oficina de Racionalización y Estadística del Ministerio Público, de los cuales se pudo advertir que el 48% (10340) fue por denuncias policiales registrados en el Distrito Fiscal de Lima y otro 35% (7668) fue registrado en siete Distritos Fiscales: Lima Norte (7%), La Libertad (5%) y Lambayeque (4%), Callao (3%) y Lima Sur (3%), lo cual denota una concentración de 83% de los delitos informáticos en ocho distritos fiscales desde octubre de 2013 a julio de 2020, donde además se registró en este último año exclusivamente 1116 denuncias penales por estos ilícitos en el Distrito Fiscal de Lima; sin embargo, en nuestro país las cifras signadas por el Ministerio Público solo han evidenciado que las denuncias por estos ilícitos se van incrementando aceleradamente año tras año, omitiendo que el 58% de las investigaciones fiscales de ese mismo periodo recayeron en archivo y que solo se emitieron 108 sentencias, generando una importante carga fiscal y una sensación de impunidad e inseguridad en las víctimas, respaldando esto encontramos a Ávila (2020), quien manifiesta que las entidades tengan equipos actualizados de la información del cliente.

Ahora bien ante lo expuesto se pudo plantear la siguiente interrogante, la cual recae en: ¿Cuáles son las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021?, del mismo modo se puede justificar, que se viene apreciando una gran discusión al momento de resolver las denuncias por los delitos informáticos, esta situación se origina en muchos casos ante la deficiente investigación fiscal, dicho ello ante la falta de conocimiento y dominio en la materia, sin embargo, este arduo camino ha permitido advertir que extremos son los que se deben fortalecer, argumentando ello con el objetivo general de determinar cuáles son las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021 y como específicos, analizar como la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021 y analizar como la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021.

II. Marco Teórico

Últimamente los delitos informáticos actúan como conductas delictivas que burlar los sistemas electrónicos o claves de acceso, pues en su mayoría son ocasionados por la tecnología, afectando bienes jurídicos diversos y desprotegiendo la confiabilidad de los datos, por ello el Estado interviene a través del Ministerio Público y con apoyo de la División de Investigación de Delitos de Alta Tecnología para poder evitar la desprotección electrónica de los mensajes, correos, o información personal.

Aspectos doctrinales como estos se tomando en consideración a nivel internacional como es el caso del Español Devia (2017), quien en su investigación: *El delito informático: Estafa informática del artículo 248.2 del Código Penal*, tesis para optar el grado académico de doctor en Derecho de la Universidad de Sevilla, aplica un diseño descriptivo a través del análisis documental, llegando a la conclusión que el avance tecnológico en el mundo ha traído consecuencias nefastas donde los delitos informáticos requieren de una nueva regulación gubernamental y mundial, para que los juzgadores tengan la instrucción suficiente de poder entender el mundo virtual y las características principales de la informática, con el fin de poder legislar adecuadamente bajo los nuevos parámetros tecnológicos.

Por consiguiente, en Colombia, Ospina y Sanabria (2020), en su investigación titulada: *Desafíos nacionales frente a la ciberseguridad en el escenario global*: un análisis para Colombia, tesis para optar el grado de doctor de la Universidad Militar Nueva Grada, aplica un diseño analítico concluyendo que el Estado Colombiano presenta diversas amenazas cibernéticas, sin embargo la pandemia Covid-19, ha generado un aumento significativo de estos delitos ya sea contra el Estado, las organizaciones o las personas, ante ello el autor requiere promover políticas sólidas de seguridad para proteger la información de las personas y las organización, esto se plantea a través de nuevas reglas del uso de software, el fomento de las denuncias y la penalización de los delitos informáticos frente a su nueva evolución.

Así mismo Hernández (2019), en su investigación titulada: *La suplantación de identidad cibernética en el Ecuador*, tesis de maestría en derecho informativo y de las nuevas tecnologías de la Universidad Externado de Colombia, aplica la metodología

descriptiva para poder identificar en que momentos se presenta la suplantación de identidad cibernética en el estado ecuatoriano, concluyendo que a pesar de que ecuador es un país subdesarrollado, la población no cuenta con la educación necesaria para establecer que tipo actos cibernéticos son considerados como delitos, ante ello el autor requiere que el gobierno plantee una campaña en donde los habitantes tengan conocimiento sobre los perjuicios y los beneficios del mundo digital, así mismo plantea que los derechos no sean actuados de una manera temporal, sino que se apliquen a un largo plazo, para alegar la sanción de un delito cometido a través de internet.

Por lo tanto, en el Salvador autores como Aguirre y Sevillano (2018), en su investigación titulada: *Desafíos a enfrentar en la aplicación de leyes sobre delitos informáticos en el Salvador*, tesis para optar el grado de maestro en seguridad y gestión de riesgos informáticos de la Universidad Don Bosco, aplica un diseño descriptivo a través del análisis documental, concluyendo que el Salvador ha desarrollado nuevos medios que permiten sancionar e investigar todo tipo de delito informático, sin embargo estos mecanismos no han podido ser apropiado para los profesionales que se dedican a la investigación tecnológica, es por ello que el autor requiere que se apliquen programas de capacidad que involucren un razonamiento del peritaje informático, para lograr concientizar el efecto e impacto de los delitos informáticos en la sociedad.

A su vez en ecuador, Ochoa (2021), en su investigación titulada: *Desafíos globales del cibercrimen Caso Ecuador período 2014 – 2019*, maestría en relación internacional de la Universidad Andina Simón Bolívar, aplica un método analítico frente a las definiciones conceptuales del ciberdelito, concluyendo que dentro del cuerpo legislativo el ciberdelito es un fenómeno global que afecta la seguridad informática y la protección de datos privados o confidenciales, pues a pesar de que existe una normativa que regular el cibercrimen, aun no es suficiente la mitigación de este tipo de delitos, debido a que no existe una política doméstica que regule adecuadamente dichos delitos, ni mucho menos los actos ilícitos que se presentan ante la vulnerabilidad de los datos personales, no obstante, el autor requiere que se aplique

un programa que brinde medidas y políticas que ayuden al sector público y privado sobre los alcances de la ciberseguridad dentro del Estado ecuatoriano.

De igual modo el autor ecuatoriano Rodríguez (2018), en su investigación titulada: *Metodología de clasificación de delitos informáticos en redes sociales su tipificación según las leyes del Ecuador*, determinación de vacíos legales y el proceso para propuesta de ley, tesis para optar el título de magister en tecnologías de la información con mención en seguridad de redes y comunicación de la Universidad Internacional Sek, el trabajo aplica un método exploratorio y descriptivo a través del instrumento de la encuesta, concluyendo que las redes sociales son las principales causas del crecimiento de ciberdelincuentes, donde consecuentemente se requiere aplicar un mejor manejo legal para validar la posibilidad de que la sociedad civil tome la iniciativa de reformar la ley frente a los delitos cibernéticos, finalmente de acuerdo a las tablas analizadas el 67.6% requieren que los delitos cometidos por redes sociales sean sancionados, es por eso que se recomienda desarrollar una nueva ley complementaria que ayude a manejar de manera jurídica los vacíos legales que presenta la norma.

De ello se puede inferir que a nivel nacional, autores como Pardo (2018), en su investigación titulada: *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018*, tesis para optar el grado de maestro en Derecho Penal y Procesal Penal de la Universidad Cesar Vallejo, teniendo como tipo el diseño descriptivo a través de la aplicación de la técnica de entrevista, donde concluye que los delitos informáticos dentro del tratamiento jurídico penal comprende todo tipo de modalidad de fraude informático, sin embargo, los delitos informáticos contra el patrimonio en su modalidad de estafa no contienen una sanción efectiva dentro del código, por tal motivo se determina que la ley informática no está totalmente actualizada de acuerdo a las nuevas modalidades cibernética.

Por otra parte Blossiers (2018), en su investigación titulada: *El delito informático y su incidencia en la empresa bancaria*, tesis para optar el grado académico de maestro en derecho empresarial, el autor aplica un método dogmático y un diseño documental, concluyendo que los delitos informáticos han impactado dentro del ámbito económico y social generando un cambio dentro de la estabilidad

jurídica, como son las pérdidas para las empresas y los activos, por ello frente al desconocimiento de la norma es necesario la aplicación de un sistema multiregulatorio penal que especialice a jueces y fiscales en delitos cibernéticos.

Del mismo modo, Machicao (2019), en su investigación titulada: *Análisis de riesgo y políticas de seguridad de información de la oficina de tecnologías de información (OTI) – una Puno 2018*, tesis para optar el grado académico de magister scientiae e informática con mención en tecnología de la información y comunicaciones de la Universidad Nacional del Altiplano, establece como método de investigación un diseño experimental a través del instrumento de la encuesta, concluyendo que la Oficina de Tecnologías de Información ha presentado un promedio de 12 riesgos informáticos que amenazan la información que administra la OIT, ante ello requiere que el Estado garantice una mejor confiabilidad, integridad y disponibilidad, pues de esta manera se ayudara a controlar la seguridad y el manejo de la información interna.

Finalmente para Tenorio (2018), en su investigación titulada: *Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia*, tesis desarrollada a través del programa de maestría en diplomacia y relaciones internacionales, aplica un diseño descriptivo a través del análisis documental, llegando a concluir que existen nuevas modalidades informáticas que evolucionan con el tiempo y generan pérdidas económicas y daños sociales a través del mal uso de las tecnologías y de los software, sin embargo para poder combatirlo plantea que el Estado coopere de manera internacional con otras materias jurídicas tomando como referencia el Convenio de Budapest con el fin de establecer responsabilidad penal a las personas involucradas.

De acuerdo a lo mencionado por los autores, se analizan como teorías relacionas al tema, aspectos doctrinales de la naturaleza del sistema informático, definiendo que en el ámbito peruano se comprende una naturaleza física y corpórea basada en el bien inmueble, pues dentro de esta automatización se ve que la valoración económica ha sido afectada dentro de las industrias, empresas, comercios por los delitos informáticos, sin embargo estas empresas siendo aún pieza fundamentales para los activos de la sociedad están siendo perjudicadas por acciones que no están debidamente reguladas como delitos (Galgano, 2005).

Así mismo se toma como concepto que el delito informático es un término que es muy usado para definir conductas que afectan el uso de la informática y las nuevas tecnologías, así como también la vulneración a los diversos bienes jurídicos, pues como se ha podido apreciar muchos de estos delitos que se utilizan afectan el principio de legalidad ya que vulnera la ley informática a través de los nuevos medios delictivos y las nuevas conductas, pues cada día con el avance de la tecnología se han presentado, nuevos medios de vulneración tecnológica (Steven, 2020).

Tal es así que Sieber (1992), menciona que este tema es uno de los temas más tomados a nivel mundial, donde se le denomino "computer crime", este medio llegó a iniciarse en periodos de los años 60 en donde se vio un incremento sobre la literatura científica , sin embargo más adelante en la reunión de la OECD se tuvo en el año de 1983 se aceptó por definir al computer crime como un computer related crime llevándolo al español comprendía que la criminalidad informática pasó a ser como una criminalidad tecnológica.

Esto nos ayuda a comprender que el delito informático a nivel del tiempo se ha usado de una manera coloquial es decir a través de la conducta que genera la informática y el avance significativo, por ende, durante estos años se facilita incrementar otros tipos de delitos como es el delito de estafa a través de internet o el delito de pornografía infantil.

Por su parte Mörhreschlager (1994), ayuda a reconocer de manera adecuada cuáles son las conductas que se presentan dentro de la criminalidad informática afirmando que actualmente no hay una definición legal acerca de qué es un delito informático sin embargo para el autor, Mörhreschlager citando a Wasik, menciona que el uso de la informática a pesar de que haya sido realizado a través de una computadora no cambia el hecho de ser un delito, ya que igual genera perjuicio a la sociedad.

De igual forma lo menciona Reyna (2012), expresa que los delitos denominados computacionales son aquellos delitos que se ejercen a través del uso de una computadora mientras que en el caso de los delitos informáticos son aquellos que afectan netamente a un bien jurídico.

De esta manera de considera que se puede denominar a un delito informático como aquel acto o conducta que afecta a un bien jurídico en concreto ya que actualmente este delito como tal no está debidamente protegido por el código penal sino por una ley especial, no obstante este delito viola la seguridad y la intangibilidad de los datos almacenados ya que estos datos no pueden ser ni transmitidos ni tratados de manera informática, en este caso se estaría hablando que el delito informático cuando es considerado como un delito autónomo pues consecuentemente el uso de las computadoras y de la tecnología constituye a que este delito afecte a bienes jurídicos tutelados denominándolo como delito informático (Recio, 2012).

Ahora con respecto a esta figura del delito informativo el derecho penal lo define como un concepto muy amplio y complejo debido a que no sólo afecta el derecho en general sino también el derecho penal, es así que se define de acuerdo al artículo 1 de la ley de delitos informáticos como todo dispositivo aislado o conjunto que se encuentra conectados o relacionados que afecta elementos y tratamientos electrónicos a través de datos o programas de ejecución (Dass, 2019)

Por ende, se presentan como características propias, según Neyra (2010), la complejidad tecnológica, el programa invasivo, sistema informático como un bien físico, alta tecnología, programas informáticos, elemento subjetivo, acopio de medios probatorios, sofisticación del cibercrimen, entre otras características que si bien es cierto son propias del sistema informático; sin embargo, la protección de los bienes jurídicos tiene que darse sobre el aspecto jurídico de protección y no sobre un bien jurídico individualizado.

Al verificar esta lesión actual, se analiza que el uso de la informática desprotege el interés jurídico pues amenaza con poder vulnerar el bien jurídico penal, así como también el nuevo realce de la tecnología de los sistemas informáticos ya que afectan bienes jurídicos tutelados y lesiona aquellos objetos que no se encuentran tutelados por el código penal; de igual forma según el autor Peña (2016), los delitos informáticos tienen que tener un interés y requisitos de necesidad para poder ser reconocidos a través del derecho y poder evaluar la categorización de vulneración del bien jurídico penal.

Esto quiere decir que con el avance de la tecnología y los nuevos medios informáticos que se presentan dentro del estado peruano que se ven que vulneran los bienes jurídicos penales, los cuales necesitan y merecen una mejor protección sin embargo haciendo énfasis en la legislación constitucional se ha venido regulando una serie de normas que, de alguna manera, han normado el manejo del uso de la tecnología de la información, en ese sentido se hayan diversas normas interpuestas dentro del estado, tal es así que la actual norma Ley 30171, la cual tipifica conductas que vulneran el bien jurídico.

Entonces se puede deducir que, en el Perú, mediante la ley, se busca prevenir conductas ilícitas así también como sancionarlas para que ya no sigan afectando a los sistemas o a los datos informáticos de las personas pues lo que se tiene que generar es una protección a los bienes jurídicos penales ya que el mayor uso de la tecnología actualmente está generando diversas vulneraciones a la información, la comunicación ya la lucha contra la ciberdelincuencia, queda claro entonces que los bienes jurídicos protegidos por el estado son los sistemas y los datos informáticos además de otros que tienen relevancia penal tal cómo es la fe pública y el patrimonio, etc. (Martínez y Serrano, 2007).

Por consiguiente, desde su análisis el bien jurídico a través de la vulnerabilidad de los delitos informáticos se ha discutido si es considerado como una infracción penal independiente y, en consecuencia, con un bien jurídico particular, o, si se trataba únicamente de una nueva forma o medio de comisión de delitos que ya se encontraban regulados en la ley penal.

Tal es así que según Bramont-Arias (1997), hace referencia que actualmente no hay un bien protegido por el delito informático pues la verdad no hay como tal un delito informático debido a que existen diversos métodos o conductas delictivas que afectan los bienes jurídicos y que el código penal hasta el momento no goza de una protección contra los actos ilícitos tecnológicos. Por su parte para el doctor argentino, Aboso (2006), el bien jurídico protegido sería “la información y su transmisión a través de los sistemas telemáticos”.

Por lo tanto, analizando las causas, se tiene que el origen del delito informático surge a través de un fraude, en donde este fraude informático versa en la transmisión

de datos, pues actualmente se analiza que esa transmisión de datos es más fácil de poder adquirirla ya que permite que el actor efectué diversas modificaciones desde una computadora ya sea en su propio domicilio o disponer de todo un terminal informático que transfiera datos adecuados de una computadora a otra.

De modo semejante Gonzales (2002), menciona que las transacciones financieras son unas de las informalidades que se generan a diario ya sea en el aspecto comercial o bancario pues a través de los pagos electrónicos la mayoría de personas han sido violentadas por los delitos informáticos, ya sea mediante sistemas que han sido abiertas de manera inéditas y que han violentado delitos patrimoniales y económicos.

No obstante, frente a los cambios que se han provocado sobre la digitalización o la globalización de las redes informáticas, se analiza que el Estado peruano aplica un convenio de Budapest dentro del cual se protegen actos que ponen en peligro los derechos de confiabilidad de integridad y de disponibilidad de sistemas ya que las redes y los datos informáticos de las personas se han visto vulnerados por sistemas de ciberdelincuencia (Mohamed, 2015).

En ese sentido, el Convenio es un cuerpo normativo que busca aplicar una mejor política penal para todos los miembros que se encuentren suscrito con el fin de que la sociedad se encuentre protegida por la nueva legislación informática además de cooperar de manera internacional con el fin de lograr mejores mecanismos para poder detener, prevenir y sancionar todo tipo de acto delictivo informático (Budapest, 2001).

Sin embargo, este convenio comprende analizar las técnicas y modalidades dentro del delito de fraude informático, delimitando que las técnicas utilizadas para la comisión del delito de fraude informático, están comprendidas por el diseño, introducción, alteración, borrado, supresión, clonación de datos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, en donde se destaca las Fuga de información, Acceso no autorizado, Pinchazo en línea, Simulación y Modelación, entre otros.

Además, Salinas (2013) menciona que, la transferencia electrónica es todo procedimiento que se realiza a través de un medio electrónico o instrumento telefónico

o computadora en donde se autoriza o se ordena el crédito débito a una cuenta o institución financiera. Por otro lado, tenemos el consumo o retiro con tarjetas clonadas que se realiza utilizando tarjetas de débito o de consumo previamente clonadas, usadas en centros comerciales para adquirir o consumir diversos productos los cuales son cancelados mediante estos mecanismos electrónicos, asumiendo para ello (el agente) la identidad del usuario clonado.

A su vez, la finalidad del agente será siempre obtener un beneficio o provecho ilícito a su favor o de un tercero; en el delito de fraude informático, el objeto "material" o "inmaterial" será la sustracción de dinero o documentos; la sustracción de mercancías; la sustracción de valores negociables o documentos que sirvan de soporte para el intercambio de mercancías o de dinero; la sustracción de servicios y finalmente la sustracción de software.

Al respecto Gil (2012), menciona que sociedad moderna actual con el vertiginoso avance de la ciencia y la tecnología de la comunicación y la informática, junto a sus beneficios, trajo consigo una serie de peligros que, en el campo del derecho penal, se materializan en la ciberdelincuencia a cuyas garras se exponen los usuarios al acceder a las redes sociales online, para el desarrollo de sus actividades cotidianas, delitos que por lo demás, no tienen fronteras, no exigen inmediación entre el agente y su víctima, permiten actuar en el anonimato y entre sus víctimas no distinguen estrato social, edades, credo religioso o color de piel.

Dicho de otro modo, el avance de la tecnología no sólo apoya la informática sino también a la comunicación mundial de uno más personas pues ésta expansión en las últimas décadas ha generado un nuevo paradigma socio ecológico denominándolo como delito informático, sin embargo esta nueva Revolución industrial basada en la informática no sólo genera delitos sino también permite poder almacenar, recuperar, comunicarse mutuamente, ya sea de una forma limitada e ilimitada a través del tiempo y la distancia (Wadha, et al., 2020)

De esta forma queda claro que en la tierra cada vez existen menos materiales para poder comunicarse pues el material más apto y dable es la tecnología ya que los nuevos factores sobre el conocimiento científico es la informática la comunicación la publicidad y las finanzas.

Finalmente, Anarte (2001), menciona que la criminalidad está asociada más a los medios informáticos y al internet llegando a denominársele como un ciberdelincuencia frente a los actos que vulneran datos informáticos, no obstante el mejor ejemplo que se puede dar de estos actos es la evolución de la criminalidad, ya que actualmente convivimos ante una sociedad de riesgo dónde probablemente el contexto sociológico de estudios informáticos no sólo se engloba en el riesgo de informar sino también riesgo patrimonial.

Es así que estas observaciones terminológicas analizadas resultan, al extraer cada uno de los verbos rectores propuestos por dicho convenio para la configuración del delito de fraude informático; por ello, entendemos que el delito de fraude informático, cualitativamente supera en exceso el campo normativo regulado dentro del derogado delito de hurto agravado (Congressional Rearch Servive, 2020).

En ese sentido, habiendo ubicado el delito de fraude informático como una de las modalidades del cibercrimen, se sostiene que los ciberdelitos, aunque coexistan en el tiempo con los llamados delitos informáticos, configurando una generación posterior cuyos problemas jurídicos están relacionados con las insuficiencias de la aplicación de la ley penal en el ámbito espacial de su vigencia y superar los límites de la extraterritorialidad que los mismos plantean, advirtiendo que las nuevas manifestaciones de criminalidad en el ciberespacio exigen su tratamiento jurídico penal desde una perspectiva internacional, con el fin de brindar una mayor protección al bien jurídico y los componentes lógicos del sistema informático.

III. Metodología

3.1. Tipo y diseño de investigación

El presente producto académico se desarrolló siguiendo el tipo **básico** de estudio, tomando en cuenta aspectos que van en función al propósito de la investigación, donde se busca tener mayor conocimiento acerca de los principios fundamentales, en relación a esto se analiza los hallazgos tecnológicos a través de la teoría para poder determinar las deficiencias en las investigaciones por delitos de fraude informático (Gonzales, 2009).

En relación al diseño de la investigación fue **fenomenológico**, pues se basa en un estudio experimental de la vida, tomando en cuentas sucesos que ya pasaron desde una perspectiva del sujeto, fundamentalmente analizando los hallazgos tecnológicos a través de la teoría para poder determinar las deficiencias en las investigaciones por delitos de fraude informático (Fuster, 2019).

También se siguió un enfoque **cualitativo**, en atención que se considera como una actividad sistemática orientada a profundizar el estudio de los fenómenos, mediante una actividad de recopilación de información destinada al descubrimiento y desarrollo de un conocimiento. (Sadín, 2003, p. 88, Citado en: Bisquerra, 2016, p. 72)

3.2. Categorías, subcategorías y matriz de categorización

Como **categoría de estudio** tenemos: Las investigaciones por delitos de fraude informático, el cual fue situado en el distrito fiscal de Lima, por contener un ingreso considerable en las denuncias por estos ilícitos, según el último reporte de la Oficina de Racionalización y Estadística del Ministerio Público.

Se define al fraude informático, como conductas penalmente relevantes que afectan sistemas informáticos que incluyen otros bienes jurídicos de orden económico, tales como el interés económico, la hacienda pública y el patrimonio; por lo que, presentan un indubitable carácter pluriofensivo, que se encuentra contemplado en el artículo 8º de la Ley Especial 30096 y su modificatoria Ley N° 30171. (Zevallos, 2020)

Sub categorías

La deficiente investigación fiscal en delitos de fraude informático.

La investigación fiscal es una previa audiencia preliminar, donde analizan diversos aspectos, sin embargo, se interpreta que, frente a los delitos de fraude informático, son menores los conocimientos que los especialistas tienen, esto se debe a la actualización tecnológica y la falta de capacitación (Cruz, 2020).

Falta de conocimiento y dominio en delitos de fraude informático.

Matriz de categorización

Esta matriz se encuentra ubicada en el Anexo 01.

3.3. Escenario de estudio

La investigación será realizada dentro del Distrito Fiscal de Lima, tomando como referencia el periodo 2021, se tomarán características particulares, en función a que todos los especialistas pertenezcan a la rama penal.

3.4. Participantes

Las personas que participarán dentro de la investigación será el Fiscal Adjunto Provincial, Asistente en función fiscal y Abogados, esta investigación se obtendrá a través de la recopilación del Distrito Fiscal de Lima.

Se han tomado en cuenta dos abogados especialistas en derecho penal, con el fin de poder analizar desde su punto de vista el fraude de los delitos informático y su repercusión en la legislación peruana.

Por otro lado, se considera tomar en cuenta dos Fiscales Adjuntos de las fiscalías provinciales Penales de Lima, con el fin de determinar si es que existen deficiencias en las investigaciones fiscales frente a los delitos de fraude informático.

Finalmente, se han tomado en consideración dos personas que laboran en la Asistencia en Función Fiscal de la fiscalía provincial Penal de Lima, esta selección se debe a que los asistentes de función fiscal, nos darán su punto de vista desde el

aspecto jurisprudencial con referencia a las deficiencias en las investigaciones fiscales frente a los delitos de fraude informático.

Tabla 1

Caracterización de participantes

Participantes	Descripción
Jesús Víctor Huamán Ortega	Abogado
Haddad Juseff Chaname Vásquez	Abogado
Clarita Judith Flores Borja	Fiscal Adjunto Provincial Penal de Lima
Jhean Franco Cifuentes Dávila	Fiscal Adjunto Provincial Penal Titular de Lima
Jeferson Rivero Guisado	Asistente en Función Fiscal - Fiscalía Provincial Penal de Lima

3.5. Técnicas e instrumentos de recolección de datos

La técnica que se utilizó en la presente investigación es la **entrevista**, por ser una técnica de recolección de datos, que permite extraer por medio de una serie de preguntas elaboradas en un esquema ordenado la opinión de los sujetos participantes. (Hernández, 2018)

Por tanto, el instrumento que permitirá una adecuada recolección de información es la **guía de entrevista**, la misma que faculta al entrevistado un margen amplio de respuesta. (Hernández, 2018)

Tabla 2

Propósito de técnicas e instrumentos

Técnica	Instrumento	Propósito
Entrevista	Guía de Entrevista	Recoger información directa de los expertos en la materia.

3.6. Procedimiento

En relación al procedimiento de recolección de data e información, se utilizó la técnica de entrevista en toda su esencia, con su respectivo instrumento, la guía de entrevista; ahora bien, las referidas entrevistas fueron aplicadas virtualmente a cinco (05) sujetos de estudio, entre los cuales tenemos a dos fiscales adjuntos provinciales, un asistente en función fiscal del Distrito Fiscal de Lima y dos abogados que desde su perspectiva externa brindaron un aporte crucial a la investigación; por otro lado, una vez recabados en su totalidad fueron incorporados en formato PDF en el apartado de anexos de este producto académico. Posteriormente fue pilar para la elaboración de la matriz de triangulación de datos adjuntos al presente estudio fenomenológico, los mismos que fueron contrastados con el análisis teórico que enriquecieron a la discusión, logrando de esta forma resultados más completos. (Hernández, 2018)

3.7. Rigor científico

Los criterios de rigor científico, ilustran paradigmas en relación al estudio de la investigación, teniendo en cuenta que se aceptan axiomas que vayan en conformidad de lo planteado y siguiendo las bases de indagación naturales, ante estos paradigmas, se analiza lo manifestado por Arias y Giraldo (2011):

Fiabilidad: permite analizar la estabilidad que tienen los resultados en función al tema planteado, tomando en cuenta el aporte de los expertos especialistas en el tema.

Dependencia: se denomina también confiabilidad cualitativa o consistencia lógica, el estudio cualitativo se encuentra sustentado con los instrumentos y técnicas de recogida de información.

Transferibilidad: permite obtener un resultado a través del desarrollo o profundización en el conocimiento en relación al problema establecido, y de esta forma lograr alcanzar el objetivo de investigación.

Confortabilidad o audibilidad: clasifica y analiza el resultado e interpretación de datos codificados en aras de una respuesta a la problemática materia de estudio.

3.8. Método de análisis de la información

Estando a la información recabada, el método de análisis aplicado en este estudio fue triangulo de datos, el mismo que busca usar diferentes estrategias y fuentes de investigación a fin de compararlo y llegar a información consolidada. (Hernández, 2018)

El cual se estructuro de la siguiente forma: **(i)** se planifico y estructuro la elaboración del instrumento (guía de entrevista) para la obtención de la data; **(ii)** ejecución en campo de estudio del referido instrumento; **(iii)** Codificación de información, la cual consistió en la incorporación y transcripción al texto de la data obtenida; **(iv)** Análisis de la información recabada y plasmada en la técnica de la triangulación donde se contrastaron las respuestas de los sujetos entrevistados (05) desde sus distintas perspectivas en un contexto de un análisis cualitativo.

3.9. Aspectos éticos

Con respecto a la investigación científica y tecnológica se tiene en cuenta que, dentro de los aspectos éticos, se toman como referencias principios y valores que vayan en conformidad a la investigación presentada, observando conductas desde el campo de la ciencia, a través del uso de carácter específicamente humano. Universidad Tecnológica de Investigación Científica – UTIC (2019)

El presente trabajo, tiene como aspectos éticos lo siguiente: 1) La autorización y validación del instrumento por la institución para su aplicación; 2) La veracidad de la información analizada, 3) La credibilidad de las opiniones realizadas en las entrevistas, mismas que se demuestra con su consentimiento y autorización y 4) El respeto de la autoría dispuestas en el Decreto Legislativo N° 822 y su modificatoria en la Ley 30276, a través de citas y referencias al estilo APA.

IV. Resultados y discusión

Con relación a la descripción de los resultados recabados, han sido presentados a través del instrumento planteado que es la guía de entrevista, donde las opiniones de los sujetos de estudio, (02) dos fiscales adjuntos provinciales, (01) un asistente en función fiscal y (02) dos abogados defensores, han permitido que se logre determinar desde su punto de vista cuales son las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima, conforme a lo detallado en lo siguiente:

De acuerdo al **objetivo general** el cual busca determinar cuáles son las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021, encontramos:

Que en relación al interrogante número uno la cual busca determinar cuáles son las deficiencias en las investigaciones fiscales por delitos de fraude informático en función a la Ley 30171, las respuestas planteadas por los especialistas entre ellos fiscales adjuntos provinciales, asistente en función fiscal y abogados defensores, se tuvo que:

La principal deficiencia de la investigación fiscal es la falta de capacitación a los sujetos procesales como es el caso de la Policía Nacional, Ministerio Público y servidores públicos, principalmente porque no se logra identificar a los presuntos autores del delito y la vinculación de este delito con la consumación del tipo penal, pues esto se genera por la falta de dominio de investigación y los vacíos legales existenciales.

Por otro lado, en el interrogante número dos, respecto a si estas deficiencias se deben a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales, los especialistas definen que:

Se debe a la mala capacitación, principalmente de la Policía Nacional, ya que ella conjuntamente con el Ministerio Público, son los dos organismos encargados de brindar investigación sobre este tipo de delitos, sin embargo, la norma queda en segundo aspecto debido a que hasta la fecha no se han incrementado nuevos delitos ni tomado en cuenta el avance tecnológico.

Entonces al hacer una conclusión de ambas respuestas se tiene que frente a las deficiencias de las investigaciones se determinan que una de las principales

deficiencias es la falta de capacidad que se tiene ante los casos delitos informáticos por parte de la Policía Nacional, el Ministerio Público y los servidores públicos principalmente cuando se logra identificar a los presuntos autores del delito y a la vinculación de este delito con el tipo penal, de esta manera se analiza qué otra medida deficiente, es la falta de actualización normativa ya que hasta la fecha no se han incrementado los nuevos delitos ni se han tomado en cuenta el avance tecnológico.

Consecuentemente al proponer el **primer objetivo específico** analizar como la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021, se planteó que:

En función a la interrogante número tres, la cual busca determinar a qué se debe la existencia de una deficiente investigación fiscal con relación a los delitos informáticos, se tuvo como respuesta que la deficiencia de la investigación fiscal en los delitos informáticos, se debe a la falta de operatividad de la Unidad de Investigación que se avoca a los delitos de Alta Tecnología (DIVINDAT) y la carga procesal de la Policía Nacional y el Ministerio Publico, así como la falta de herramientas para poder identificar e individualizar al autor o autores de los delitos informáticos.

Del mismo modo con la interrogante número cuatro, cual busca sabes si la deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática, se tiene que sí, debido a que existen nuevos medios de criminalidad tecnológicos, que no se encuentran regulados en la norma, ni recoge las nuevas actualizaciones de fraude, pues estos tipos de conductas, deben de aplicarse en función a que se contrarresten la criminalidad informática y la sanción del autor mismo.

Así mismo, al plantear la interrogante cinco en función a qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático, se determinó que se debe de brindar una mejor capacitación en función a los nuevos delitos y la actualización normativa, implementando equipos tecnológicos que vayan de acuerdo la vanguardia del Siglo XXI y logren identificar el IP ante las denuncias recibidas de fraude informático.

Concluyendo que las deficiencias se la investigación fiscal se presentan por la falta de capacidad, operativa de la Unidad de Investigación que se avoca a los delitos

de Alta Tecnología (DIVINDAT) y la carga procesal de la Policía Nacional y el Ministerio Publico; sin embargo, estas deficiencias perjudican a que se realicen efectivamente las investigación por delito informativo, debido a que con el avance de la tecnología esto genera de que los nuevos delitos de criminalidad no se encuentren regulados en la propia norma, ni bajo las nuevas actualización de fraude, pues muchas veces se evitan contrarrestar criminalidad informática, y determinar el tipo de conducta del autor.

Finalmente, al plantear el **segundo objetivo específico,** el cual busca analizar como la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021.

Se tuvo que por parte de los especialistas el responder la pregunta número seis, respecto a si la falta de conocimiento y dominio en las investigaciones por delitos de fraude informático se debe a que la normativa no está acorde a la realidad nacional, se tiene que, sí, como bien se sabe a pesar de que la norma se encuentre establecida hace 8 años, aún existe nuevos medios tecnológicos que no se encuentran regulados en la legislación, pues incrementando un mejor control electrónico, se estaría brindando mayor capacitación a los operadores judiciales y la sanción de las normas ante las nuevas conductas fraudulentas.

Del mismo modo al responder la interrogante siete, respecto a qué se debería mejorar en la Ley de delitos informáticos, se pudo determinar que se debería incorporar nuevos artículos que involucren a un ingeniero de sistemas dentro de la investigación preliminar, así como al personal policial y al Ministerio Público, esta modificación normativa tiene que ir en función a la ciberseguridad y a las conductas aun no tipificadas, facultando un mejor control tecnológico y fiscalizando el acceso al secreto de las comunicaciones.

Del mismo modo bajo la última interrogante la cual busca determinar qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático, se tuvo como respuesta que debería existir una previa coordinación con ambas entidades, así como tener las herramientas adecuada para poder identificar el uso de las tecnologías y fraude informático, finalmente se debe tomar en cuenta los plazos y las acciones de

investigación ante este tipo de casos, generando una mejor confiabilidad, integridad y disponibilidad de los datos de la víctima.

Concluyendo que tanto la falta de conocimiento como la falta de dominio dentro de la investigación se debe a que existe una mala aplicación normativa, ya que a pesar de la norma establecida aún no se presentan los nuevos medios tecnológicos, con el fin de incrementar un mejor control electrónico y una mayor capacitación jurídica a los operadores de justicia, asimismo se establece que la actual ley de delitos informáticos debería aplicar nuevos artículos que involucren una mejor ciberseguridad, pues las medidas aplicadas por el Ministerio Público y la Policía Nacional no son eficazmente relacionados con los delitos, es por eso que entre ambas entidades debe existir una mejor coordinación para brindar medidas adecuadas que ayuden a identificar el uso de las tecnologías y el fraude informático brindando una mejor confiabilidad, integridad y disponibilidad ante los datos de la víctima.

De acuerdo a los resultados expuestos se puede discutir la investigación de la siguiente manera:

Respecto al **objetivo general**: Determinar las deficiencias de las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021.

Con respecto a la entrevista aplicada, se toma en cuenta que en función al objetivo general que busca determinar las deficiencias de las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021, aplicada al fiscal adjunto provincial, asistente en función fiscal y abogados defensores, quienes mencionan que una de las principales deficiencias es la falta de capacidad que se tiene ante los casos delitos informáticos por parte de la Policía Nacional, el Ministerio Público y los servidores públicos principalmente cuando se logra identificar a los presuntos autores del delito y a la vinculación de este delito con el tipo penal, esta respuesta es mencionada de acuerdo a la pregunta 1, pues se interpreta que el principal problema es la falta de capacitación por parte del Ministerio Público, así como los vacíos legales que se presentan por la no actualización de la norma conforme a los nuevos fraudes tecnológicos.

De esta manera se analiza qué conforme a la pregunta 2 planteada entre la falta de capacidad y la mala aplicación normativa, la falta de capacidad es una de las

principales deficiencias que se tienen por parte del Estado ante los órganos judiciales, pues es parte tanto del Ministerio Público como de la PNP, coordinar ante esta clase de delitos, sin embargo, como segundo supuesto la falta de actualización normativa hasta la fecha no se han incorporado las nuevas modalidades ni se han tomado en cuenta el avance tecnológico.

Conforme a lo mencionado se establece que la falta de capacitación del Estado hacia la Policía Nacional, el Ministerio Público y los servidores públicos, con respecto a los delitos cibernéticos, generan que se presenten deficiencias de investigación en función a estos delitos informáticos, pues en muchas ocasiones se ha presentado que los delitos actuales de fraude informático no se encuentran aún regulados en la norma, generando así que los mismos organismos de protección no vengan conociendo sobre los elementos típicos, ni la consumación del delito.

Esto guarda relación de acuerdo a lo mencionado por Aguirre y Sevillano (2018), quien, concluyendo que el Salvador ha desarrollado nuevos medios que permiten sancionar e investigar todo tipo de delito informático, sin embargo estos mecanismos no han podido ser apropiado para los profesionales que se dedican a la investigación tecnológica, es por ello que el autor requiere que se apliquen programas de capacidad que involucren un razonamiento del peritaje informático, para lograr concientizar el efecto e impacto de los delitos informáticos en la sociedad.

De acuerdo a ello se analiza que en países como el Salvador se establece brindar una mejorar capacidad de información a los organismos administradores de justicia, con el fin de dar a conocer los nuevos delitos informáticos y sus modalidades aplicables ante la actualización de la norma conforme al fraude informático y al nuevo control tecnológico.

De esta manera autores como Hernández (2019), en su investigación, concluye que a pesar de que Ecuador es un país subdesarrollado, la población no cuenta con la educación necesaria para establecer que tipo actos cibernéticos son considerados como delitos, ante ello el autor requiere que el gobierno plantee una campaña en donde los habitantes tengan conocimiento sobre los perjuicios y los beneficios del mundo digital; asimismo, plantea que los derechos no sean actuados de una manera temporal,

sino que se apliquen a un largo plazo, para alegar la sanción de un delito cometido a través de internet.

De acuerdo a lo que menciona el autor se analiza qué la población muchas veces no cuenta con los medios necesarios para poder establecer cuáles son los nuevos tipos de acto cibernético considerados como delitos, pues requiere que se aplique una nueva campaña en donde el gobierno capacite legalmente a todos sus administradores de justicia con el fin de que esta campaña busqué beneficios dentro de un mundo digital y plantee derechos que vayan conforme a la sanción del delito y a la responsabilidad ante la víctima.

En relación al **primer objetivo específico**: Analizar si deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021.

Ahora con respecto al objetivo específico uno, que busca analizar si la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021, instrumento que ha sido aplicado a través del fiscal adjunto provincial, asistente en función fiscal y por un abogado defensor, se determina que conforme a la pregunta número 3, se tiene en cuenta que se presentan deficiencias como la falta de capacidad, operativa de la Unidad de Investigación que se avoca a los delitos de Alta Tecnología (DIVINDAT) y la carga procesal de la Policía Nacional y el Ministerio Público, sin embargo estas deficiencias perjudican a que se realicen efectivamente las investigación por delito informático e individualicen al autor del delitos.

Conforme a ello se tiene de que las deficientes investigaciones fiscales si perjudican a las investigaciones por delito de fraude informático, esto se analiza conforme la pregunta 4, donde se interpreta que principalmente existe un perjuicio a las investigaciones fiscales, debido a que no cuentan con las herramientas suficientes para poder individualizar los delitos informáticos, ni mucho menos con un personal especializado que se encargue de investigar deficientemente estos delitos.

Debido al avance de la tecnología se establece que el Estado peruano debe implementar medidas que ayuden a resolver los casos de fraude informático, esto se analiza conforme lo mencionado en la pregunta 5, donde los expertos expresan que una

de las mejores medidas que pueden brindar el Estado, es la capacitación a los funcionarios públicos en función a los nuevos delitos y la actualización de la norma.

Esto se debe a que los nuevos delitos de criminalidad no se encuentren regulados en la propia norma, ni bajo las nuevas actualizaciones de fraude, pues muchas veces se evitan contrarrestar criminalidad informática, y determinar el tipo de conducta del autor.

Conforme a estas respuestas analizadas, se toma en cuenta lo mencionado por el autor Devia (2017), quien en su investigación llega a la conclusión que el avance tecnológico en el mundo ha traído consecuencias nefastas donde los delitos informáticos requieren de una nueva regulación gubernamental y mundial, para que los servidores públicos tengan la instrucción suficiente de poder entender el mundo virtual y las características principales de la informática, con el fin de poder legislar adecuadamente bajo los nuevos parámetros tecnológicos.

Este autor menciona que la falta de capacidad de los servidores públicos es una de las principales deficiencias que se tiene para poder entender el mundo informático y los delitos aplicado a ella, es con este avance tecnológico se deben de presentar nuevas actualizaciones en la norma, tomando en cuenta las características principales de la informática, con la finalidad de adecuar la norma bajo los nuevos parámetros tecnológicos.

De manera similar el autor Pardo (2018), en su investigación concluye que los delitos informáticos dentro del tratamiento jurídico penal comprenden todo tipo de modalidad de fraude informático; sin embargo, los delitos informáticos contra el patrimonio en su modalidad de estafa no contienen una sanción efectiva dentro del código, por tal motivo se determina que la ley informática no está totalmente actualizada de acuerdo a las nuevas modalidades cibernética.

Esto comprende que, a pesar la falta de capacitación existencial en los delitos informáticos, la mala comprensión normativa y la falta de actualización de la norma son otros factores que se involucran ante las deficientes investigaciones fiscales, principalmente por que la norma no se encuentra amparada bajo los nuevos lineamientos de avance tecnológico, es por ello que se requiere que la ley informática este actualizada de acuerdo a las nuevas modalidades cibernética.

Finalmente, el **segundo objetivo específico**: Analizar si la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021.

Finalmente, de acuerdo a lo que plantea el objetivo específico dos, el cual busca analizar si la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021, se obtuvo que de acuerdo a la encuesta aplica al fiscal adjunto provincial, asistente en función fiscal y abogado defensor, se establece que la falta de conocimiento y dominio si perjudican las investigación fiscales que se presentan ante el fraude información, principalmente porque se llegan a presentarse ante una mala aplicación normativa, ya que a pesar de la norma establecida hace 8 años aún se pude percibir de que los nuevos delitos y modalidades de estafa cibernética, no se encuentran debidamente regulados, conforme se analizado en la pregunta 6, se establece que se debería brindar un mejor control electrónico y una mayor capacitación jurídica a los operadores de justicia ante los nuevos medios tecnológicos.

Asimismo, se establece que de acuerdo a la pregunta 7 la actual ley de delitos informáticos debería aplicar nuevos artículos que involucren una mejor ciberseguridad, en función la ciberseguridad y a las conductas aun no tipificadas, facultando un mejor control tecnológico y fiscalizando el acceso al secreto de las comunicaciones.

Finalmente, de acuerdo a lo que establece la pregunta 8 y en concordancia con el objetivo específico dos, las medidas aplicadas por el Ministerio Público y la Policía Nacional no son eficazmente relacionados con los delitos, es por eso que entre ambas entidades debe existir una mejor coordinación para brindar medidas adecuadas que ayuden a identificar el uso de las tecnologías y el fraude informático brindando una mejor confiabilidad, integridad y disponibilidad ante los datos de la víctima.

De acuerdo a ello autores como Blossiers (2018), en su investigación concluyen que los delitos informáticos han impactado dentro del ámbito económico y social generando un cambio dentro de la estabilidad jurídica, como son las pérdidas para las empresas y los activos, por ello frente al desconocimiento de la norma es necesario la aplicación de un sistema multiregulatorio penal que especialice a jueces y fiscales en delitos cibernéticos.

Conforme a lo que hace mención el autor tanto la falta de conocimiento y dominio se debe al desconocimiento de la norma, es por ello que el autor analiza que se aplique un mejor sistema multiregulatorio penal, tomando en cuenta que los jueces y los fiscales dentro de los delitos cibernéticos deben de ejecutar una mejor capacitad ante el conocimiento de los delitos y la actualización de la norma.

De manera similar lo manifestado por Tenorio (2018), concluye que las nuevas modalidades informáticas que evolucionan con el tiempo y generan pérdidas económicas y daños sociales a través del mal uso de las tecnologías y del software, sin embargo, para poder combatirlo plantea que el Estado coopere de manera internacional con otras materias jurídicas tomando como referencia el Convenio de Budapest con el fin de establecer responsabilidad penal a las personas involucradas.

Esta es otra de las manifestaciones que se pueden presentan ante la falta de conocimiento y dominio, pues el Estado peruano con las nuevas normativas jurídicas puede tomar como referencias convenios que tienen con el fin de poder brindar una mejor seguridad jurídica con respeto a los delitos informáticos.

V. Conclusiones

Primera:

Se determina que una de las principales deficiencias, es la falta de capacidad que se tiene ante los casos delitos informáticos por parte de la Policía Nacional, el Ministerio Público y los servidores públicos, principalmente cuando se logra identificar a los presuntos autores del delito y a la vinculación de este con el tipo penal; adicionalmente otra deficiencia detectada, es la falta de actualización normativa ya que hasta la fecha no se han incorporado las nuevas modalidades ni se han tomado en cuenta el avance tecnológico.

Segunda:

Se determina que las deficiencias advertidas en la investigación fiscal se presentan por la falta de capacidad operativa de la Unidad de Investigación avocada a los delitos de Alta Tecnología (DIVINDAT) y a la carga procesal dentro de las oficinas de la Policía Nacional y el Ministerio Público; sin embargo, estas deficiencias perjudican a que se realicen efectivamente las investigaciones por este ilícito, debido a que con el avance de la tecnología se genera que los nuevos delitos de criminalidad no se encuentren regulados en la propia norma, ni bajo las nuevas actualizaciones de fraude, pues muchas veces por desconocimiento, se evita contrarrestar la criminalidad informática y la determinación del tipo de conducta del autor.

Tercera:

Tanto la falta de conocimiento como la falta de dominio dentro de la investigación se deben a que existe una mala aplicación normativa; asimismo, se establece que la actual ley 30096 de delitos informáticos, debería considerar nuevos artículos que involucren una mejor ciberseguridad, pues las medidas aplicadas por el Ministerio Público y la Policía Nacional no son eficazmente relacionados con los delitos, ello a razón que entre ambas entidades no existe una coordinación adecuada que permita

brindar mejores medidas que ayuden a identificar el uso de las tecnologías y a los autores del fraude informático denunciado.

VI. Recomendaciones

Primera:

Capacitar permanentemente a la Policía Nacional y al Ministerio Público de acuerdo a los nuevos delitos cibernéticos; asimismo, se requiere tomar en cuenta la capacitación de la actualización de la norma y la celeridad de las investigaciones fiscales que permitan una adecuada dirección de las diligencias.

Segunda:

Actualizar con una periodicidad anual la ley 30096, a fin que esta incorpore los nuevos delitos de criminalidad y delitos de fraude, para ello el estado peruano debe implementar nuevos equipos tecnológicos que ayuden al desarrollo de las investigaciones fiscales.

Tercera:

Incrementar un mejor control electrónico, tomando en cuenta la cooperación que debe existir entre el Ministerio Público y la Policía Nacional, con el fin que ambas entidades logren implementar mesas de trabajo unificado que ayuden a identificar el uso de las tecnologías y a los autores por delitos de fraude informático; y así lograr reducir la impunidad e inseguridad en las victimas.

Referencias

Aboso, E. (2006). *Cibercriminalidad y derecho penal*. Editorial Montevideo, Buenos Aires.

Aguirre, C. y Sevillano Flores, J. A. (2018). *Desafíos a enfrentar en la aplicación de leyes sobre delitos informáticos en el Salvador*, Universidad Don Bosco, recuperado de https://bit.ly/3h07Ib6

Alansari, M.; Zainab, Aljazzf y Muhammad S. (2019). *On Cyber Crimes and Cyber Security*, Researchgate, https://www.researchgate.net/publication/331914032_On_Cyber_Crimes_and_Cyber_Security

Anarte, E. (2001). *Incidence of new technologies in the penal system. Approach to criminal law in the information society*, en Universidad de Giorga,.

Arias, M. y Giraldo, C. (2011). El rigor científico en la investigación cualitativa, Revista Redalyc, https://bit.ly/3h35I1B

Ávila, S. (2020). *Fraude informático: 1771 personas han sido víctimas de los ciberdelincuentes según estadísticas de la DIVINDAT,* Perú21, recuperado de *https://bit.ly/35QEQNm*

Blossiers, J. (2018). *El delito informático y su incidencia en la empresa bancaria*, Universidad Nacional Federico Villareal, recuperado de file:///C:/Users/USER/Downloads/UNFV_BLOSSIERS_%20MAZZINI_%20JUAN%20_JOS%C3%89_MAESTRIA_2018.pdf

Bramont-Arias, L. (1997). *El delito informático en el código penal peruano*, PUCP, Lima

Budapest (2001). *El convenio sobre la ciberdelincuencia*

Castillo, M. (2020). *La ciberdelincuencia: ¿quién nos protege?*, Legis.pe, recuperado de https://bit.ly/3xMUUeT

Congressional Rearch Servive. (2020). *Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*, https://fas.org/sgp/crs/misc/R46536.pdf

Cruz, Y. (2020). *¿Cuándo el fiscal puede concluir que la investigación preparatoria ha cumplido su objeto?*, Legis.pe, https://bit.ly/3jp3Y5R

Dass, J. (2019). *Book Review of Principles of Cyber Crime*, Open Access, https://www.cybercrimejournal.com/BookReviewDassvol13issue1IJCC2019.pdf

Devia, E. (2017). *Estafa informática del artículo 248.2 del código penal*, Universidad de Sevilla, España, recuperado de https://bit.ly/2TUPgZr

Devia, E. (2017). *Estafa informática del artículo 248.2 del Código Penal*, Universidad de Sevilla, España, recuperado de https://bit.ly/3vV4Wcn

Fusrter, D. (2019). *Investigación cualitativa: Método fenomenológico hermenéutico*, Revista Educativa, https://bit.ly/2TUP4cF

Galgano, F. (2005). *La globalización en el espejo del derecho*, Buenos Aires, Rubinzal-Culzoni

Gil, A. (2012). *El fenómeno de las redes sociales y los cambios en la vigencia de los derechos fundamentales*, Revista de derecho UNED, España

Gonzales, C. (2009). *La Investigación Básica. La Investigación en Ciencias Fisiológicas: Bioquímica, Biología Molecular y Fisiología*. Cuestiones Previas, https://bit.ly/3qolhoQ

Gonzales, J. (2002). *Protección penal de sistemas, elementos, datos, documentos y programas informáticos en el derecho español*, De los delitos informáticos. Aspectos criminológicos, dogmáticos y de política criminal, ed. mes de enero, Jurista, Lima

Hernández, D. (2019). *La suplantación de identidad cibernética en el ecuador*, Universidad Externado de Colombia, recuperado de https://bit.ly/3xNMxj6

Hernández, R. (2018). *Metodología de la investigación científica*. Industria Editorial Mexicana, México,

Herrera, G. (2020). *Auge del fraude cibernético en Venezuela y otras tendencias delictivas,* Revista El diario, Venezuela, recuperado de *https://bit.ly/3xVdhOT*

Machicao, S. (2019). *Análisis de riesgo y políticas de seguridad de información de la oficina de tecnologías de información (OTI) – una Puno 2018*, Universidad Nacional del Altiplano, recuperado de https://bit.ly/3j9SFOu

Martínez, E. y Serrano A. (2007). *La evolución hacia una nueva brecha digital*. En red. Recuperado en: http://www.labrechadigital.org/.

Mayer L. (2020). *El delito de fraude informático: concepto y delimitación, Revista Chilena de Derecho y Tecnología*, recuperado de https://bit.ly/3gU0u9K

Mayer, L. y Oliver, G. (2020). *El delito de fraude informático: Concepto y delimitación*, Revista Chilena de derecho y tecnología, Chile, recuperado de file:///C:/Users/USER/Downloads/57149-913-197774-1-10-20200715.pdf

Ministerio Público (2021). *Ciberdelincuencia: pautas para una investigación fiscal especializada*, OFAEC, recuperado de https://bit.ly/2T4Bt2f

Mohamed, Ch.; Ashraf, D.; Mohammad Ayoub, K. y Sapana Tyagi (2015). *Cybercrime, digital forensics and jurisdiction*, Springer, Studies in Computational Intelligence.

Möhrenschlager, M. (1994). *Computer crimes and other crimes against information technology in Germany*, Colonia, Carl Heymans.

Neyra, J. (2010). *Manual del nuevo proceso penal*, Lima, Idemsa,

Nurse, J. (2018). *Cybercrime and You: How Criminals Attack and the Human Factors That They Seek to Exploit*, Researchgate, https://www.researchgate.net/publication/328762019_Cybercrime_and_You_How_Criminals_Attack_and_the_Human_Factors_That_They_Seek_to_Exploit

Ochoa, A. (2021). *Desafíos globales del cibercrimen Caso Ecuador período 2014 – 2019*, Universidad Andina Simón Bolívar, recuperado de https://bit.ly/3zSM2Gm

Ochoa, M. (2020). *Delitos informáticos en México, ¿qué dice la Ley?*, It Maters, México, recuperado de https://bit.ly/3jc7XCA

Ospina, M. y Sanabria, P. (2020). *Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia*, Universidad Militar Nueva Grada, recuperado de https://bit.ly/3h1lU3q

Pardo, A. (2018). *Tratamiento jurídico penal de los delitos informáticos contra el patrimonio*, Distrito Judicial de Lima, 2018, Universidad Cesar Vallejo, recuperado de https://bit.ly/2SVrlsT

Peña, D. (2016). *Delitos informáticos*, Revista virtual intercambios

Recio, M. (2012). *De la seguridad informática a la seguridad de la información*. Madrid. Edt. Gesio. p.4.

Reyna, L. (2012). *Los delitos informáticos. Aspectos criminológicos, dogmáticos y de política criminal*, Lima, Jurista

Rodríguez, C. (2018). *Metodología de clasificación de delitos informáticos en redes sociales su tipificación según las leyes del ecuador, determinación de vacíos legales y el proceso para propuesta de ley*, Universidad Internacional Sek, recuperado de https://bit.ly/2SVuIA5

Roibón, M. (2019). *La estafa informática en el Código Penal Argentino*, Revista Pensamiento Penal, Argentina, recuperado de https://bit.ly/3jbQgTu

Sandín, M. (2003). *Investigación cualitativa en educación. Fundamentos y tradiciones*. Madrid, España: Editorial Mc Graw Hill. Citado en: Bisquerra, R. (2016). Metodología de la Investigación Educativa. Madrid, España: Editorial La Muralla.

Salinas, R. (2013). *Derecho penal. Parte especial*, Grijley, Lima.

Sequera, M. y Samaniego, M. *Desafíos de la armonización de la convención de Budapest en el sistema penal paraguayo*, TEDIC, Paraguay, recuperado de https://bit.ly/3zWmgRC

Sieber, U. (1992). *IUS Informationis. The Internacional Emergence of Criminal Information Law,Colonia*: Carl Heymans.

Steven Kemp, V. (2020). Fraud against individuals in the internet era: trends, victimisation, impact and reporting, Universitat de Girona, https://www.tesisenred.net/bitstream/handle/10803/671164/tsk_20201204.pdf?sequence=2&isAllowed=y

Tantaleán, R. (2016). *Tipología De Las Investigaciones Jurídicas, Derecho y Cambio Social*, recuperado de file:///C:/Users/USER/Downloads/Dialnet-TipologiaDeLasInvestigacionesJuridicas-5456267%20(1).pdf

Tenorio, J. (2018). *Desafíos y oportunidades de la adhesión del Perú al Convenio de Budapest sobre la Ciberdelincuencia*, Programa de Maestría En Diplomacia Y Relaciones Internacionales, recuperado de https://bit.ly/3x0Zuq0

Universidad Tecnológica de Investigación Científica (2019), *Código de ética de investigación científica y tecnología*, Colombia, https://bit.ly/3vW71ES

Wadha Abdullah, A; Somaya Al-Maadeed; Abdulghani Alii, A. y Muhammad Khuraam K. (2020). C*omprehensive Review of Cybercrime Detection Techniques*, IEEE Access, https://wlv.openrepository.com/bitstream/handle/2436/623411/Sadiq_Comprehensive_Review_of_Cybercrime_2020.pdf?sequence=6&isAllowed=y

Zevallos, O. (2020). *Delitos informáticos: ¿Cuáles son los principales fraudes informáticos que se pueden cometer a través del E-Commerce?*, Ius 360, https://bit.ly/35TxPLD

ANEXOS

Anexo 1: Matriz de categorización								
Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021								
FORMULACION DE PROBLEMA	**OBJETIVO GENERAL**	**CATEGORIA**	**SUBCATEGORIAS**	**OBJETIVOS ESPECIFICOS**	**SUJETOS INFORMARTES**			**ENTREVISTAS / PREGUNTAS**
P.G.: ¿Cuáles son las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021?	Determinar las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021	Las investigaciones por delitos de fraude informático			Fiscal Adjunto Provincial	Asistente en Función Fiscal	Abogado	1 ¿Cuáles considera usted que son las deficiencias en las investigaciones fiscales por delitos de fraude informático en función a la Ley 30171? 2 En referencia a la pregunta anterior. ¿Estas deficiencias se deben a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?
P.E.1: ¿Cómo la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021?			La deficiente investigación fiscal en delitos de fraude informático	Analizar como la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021				4 ¿A qué se debe la existencia de una deficiente investigación fiscal con relación a los delitos informáticos? 5 ¿La deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática? 6 ¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático?
P.E.2: ¿Cómo la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021?			Falta de conocimiento y dominio en delitos de fraude informático	Analizar como la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021				7 ¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático se debe a que la normativa no está acorde a la realidad nacional? 8 ¿Qué se debería mejorar en la Ley de delitos informáticos? 9. ¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático?

Anexo 02 – Matriz de triangulación

Matriz de triangulación del objetivo general

OBJETIVO GENERAL			
O.G. Determinar cuáles son las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021	**S1. FISCAL ADJUNTO PROVINCIAL**	**S2. ASISTENTE EN FUNCION FISCAL**	**S3. ABOGADO**
P1. OG ¿Cuáles considera usted que son las deficiencias en las investigaciones fiscales por delitos de fraude informático en función a la Ley 30171?	El problema fundamental radica en la muy difícil capacidad para lograr identificar objetivamente a los presuntos autores de estos delitos y, a su vez vincularlos con los elementos típicos para la	Se debe principalmente a la falta de capacitación tanto a los funcionarios y servidores públicos de los órganos jurisdiccionales; lo que causa una falta de dominio de investigación y una mala aplicación de la norma en perjuicio del bien	Considero que existe deficiencias en las investigaciones por falta de capacitación de los diferentes sujetos procesales como la Policía, el Ministerio Público y los jueces, toda vez que estos delitos tratan sobre

	consumación con el tipo penal.	jurídico protegido; sumado a ello, se debe tener en cuenta los vacíos legales que existen y que no protegen ciertas conductas en cuanto a la criminalidad tecnológico que cada día es más frecuente.	tecnologías nuevas por lo sé que se requiere una constante capacitación además de una legislación acorde.
ANÁLISIS	La principal deficiencia de la investigación fiscal es la falta de capacitación a los sujetos procesales como es el caso de la Policía Nacional, Ministerio Publico y servidores públicos, principalmente porque no se logra identificar a los presuntos autores del delito y la vinculación de este delito con la consumación del tipo penal, pues esto se genera por la falta de dominio de investigación y los vacíos legales existenciales.		
P2. OG ¿Estas deficiencias se deben a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?	Se debe a la falta de capacitación por parte del Estado a los órganos policiales, mas no a los judiciales. Hago esa precisión puesto que, los juzgados no "investigan", sino el Ministerio Público en	Considero que se debe a ambas, debido a que por una parte, al existir ciertos vacíos legales, la norma no regula correctamente los nuevos delitos cibernéticos que a la fecha se han incrementado, ni mucho	Además de la falta de capacitación, existe una falta de personal especializado en la Policía y Ministerio Publico, que puedan y resuelvan estos

	directa coordinación con la PNP especializada para esta clase de delitos.	menos toma en cuenta el avance tecnológico; por otra parte, el personal de los órganos judiciales no están debidamente capacitados por el Estado a efectos de poder conducir una adecuada y correcta investigación ante los nuevos casos de fraude informático del cual muchas personas son víctimas de estos delitos.	casos con la celeridad que se requiere
ANÁLISIS	Se debe a la mala capacitación, principalmente de la Policía Nacional, ya que ella conjuntamente con el Ministerio Publico, son los dos organismos encargados de brindar investigación sobre este tipo de delitos, sin embargo, la norma queda en segundo aspecto debido a que hasta la fecha no se han incrementado nuevos delitos ni tomado en cuenta el avance tecnológico.		
CONCLUSIÓN	Frente a las deficiencias de las investigaciones se determinan que una de las principales deficiencias es la falta de capacidad que se tiene ante los casos delitos informáticos por parte de la Policía Nacional, el Ministerio Público y los servidores públicos principalmente		

	cuando se logra identificar a los presuntos autores del delito y a la vinculación de este delito con el tipo penal, de esta manera se analiza qué otra medida deficiente, es la falta de actualización normativa ya que hasta la fecha no se han incrementado los nuevos delitos ni se han tomado en cuenta el avance tecnológico.

Matriz de triangulación del objetivo específico 1

OBJETIVO ESPECIFICO 1			
O.E.1 Analizar si la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021	**S1. FISCAL ADJUNTO PROVINCIAL**	**S2. ASISTENTE EN FUNCIÓN FISCAL**	**S3. ABOGADO DEFENSOR**
P1. OG1 ¿A qué se debe la existencia de una deficiente investigación fiscal con	La deficiencia en las investigaciones fiscales respecto a los delitos informáticos obedece básicamente a la falta de	Esto se debe a que las investigaciones preliminares no tienen un valor normativo ni judicial, debido a que los nuevos	Debemos considerar que la Policía Nacional y el Ministerio Publico presenta una alta carga procesal en delitos contra el patrimonio,

relación a los delitos informáticos?	operatividad por parte de la Unidad de Investigación que se avoca a los delitos de Alta Tecnología (DIVINDAT), ya que estos casos no se pueden llevar a cabo en “sede fiscal”, dado que, en un despacho no se cuenta con equipos sofisticados para ello, sino todo lo contrario.	alcances de modalidad de fraude informático tecnológico no se encuentren actualizados en la norma, ni en la capacitación de los juzgadores, es más, tanto la Fiscalía como la Policía Nacional del Perú no siempre cuentan con las herramientas suficientes a fin de poder identificar e individualizar al autor o autores de los delitos informáticos.	además la falta de personal especializados hace que las investigaciones en delitos informáticos sean deficientes.
ANÁLISIS	La deficiencia de la investigación fiscal en los delitos informáticos, se debe a la falta de operatividad de la Unidad de Investigación que se avoca a los delitos de Alta Tecnología (DIVINDAT) y la carga procesal de la Policía Nacional y el Ministerio Publico, así como la falta de herramientas para poder identificar e individualizar al autor o autores de los delitos informáticos.		

P2. OG1 ¿La deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática?	No considero que existan vacíos legales para el tipo penal de Fraude informático, ya que la Ley Especial con la cual se incorporó este delito y otros de naturaleza similar, desarrollan correctamente el alcance de sus verbos rectores, sin embargo, sí considero que existe una escasez de normativa.	Considero que sí, dado que los nuevos medios de fraude tecnológico en su totalidad, aún no se encuentran regulados en la norma penal, por consiguiente, dichas conductas no tienen una pena establecida que coadyuve a poder contrarrestar estos nuevos delitos en función a la criminalidad informática, así como sancionar a los autores del mismo.	Los delincuentes informáticos hacen uso de tecnológicas novedosas por lo que es necesario una legislación acorde a esta realidad. Si bien tenemos la ley 3071, esta legislación no recoge todas las actualidades modalidades de fraude informático, por lo que el Estado debería incorporar nuevos tipos penales.
ANÁLISIS	Si, debido a que existen nuevos medios de criminalidad tecnológicos, que no se encuentran regulados en la norma, ni recoge las nuevas actualizaciones de fraude, pues estos tipos de conductas, deben de aplicarse en función a que se contrarresten la criminalidad informática y la sanción del autor mismo.		

P3. OG1 ¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático?	El Estado peruano debería brindar mayor implementación de equipos tecnológicos a la vanguardia del Siglo XXI, los cuales permitirían una mejor investigación respecto a naturaleza de ese delito	Definitivamente se debe capacitar a los funcionarios y servidores de los órganos jurisdiccionales, ello a efecto sé que pueden tener un mejor panorama jurídico en cuento a los delitos informáticos; asimismo, tanto los legisladores como los magistrados deben de actualizar, así como analizar a mayor profundidad la norma aplicable a los delitos informáticos. Aunado a ello, el Estado debe brindar programas de orientación a la ciudadanía y poder llevar un mejor control de confiabilidad.	Primero, se debe establecer protocolos de acción inmediata que permitan identificar de manera rápida a los delincuentes informático. La policía debe contar con herramientas tecnológicas para identificar los IP ni bien reciba la denuncia.

ANÁLISIS	Debe de brindar una mejor capacitación en función a los nuevos delitos y la actualización normativa, implementando equipos tecnológicos que vayan de acuerdo la vanguardia del Siglo XXI y logren identificar el IP ante las denuncias recibidas de fraude informático.
CONCLUSIÓN	Se determina que las deficiencias se la investigación fiscal se presentan por la falta de capacidad, operativa de la Unidad de Investigación que se avoca a los delitos de Alta Tecnología (DIVINDAT) y la carga procesal de la Policía Nacional y el Ministerio Publico, sin embargo estas deficiencias perjudican a que se realicen efectivamente las investigación por delito informativo, debido a que con el avance de la tecnología esto genera de que los nuevos delitos de criminalidad no se encuentren regulados en la propia norma, ni bajo las nuevas actualización de fraude, pues muchas veces se evitan contrarrestar criminalidad informática, y determinar el tipo de conducta del autor.

Matriz de triangulación del objetivo específico 2

OBJETIVO ESPECIFICO 2			
O.E.2 Analizar si la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021	**S1. FISCAL ADJUNTO PROVINCIAL**	**S2. ASISTENTE EN FUNCIÓN FISCAL**	**S3. ABOGADO DEFENSOR**
P1. OG2 ¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático se debe a que la normativa no está acorde a la realidad nacional?	Si bien es cierto, los delitos informáticos en general (no específicamente el "fraude informático") se encuentran regulados hace aproximadamente 08 años atrás, resulta que desde ese entonces era de carácter simbólico en el Código Penal, ya que con su	Opino que sí, pues para ello se tiene que basar en las nuevas herramientas tecnológicas, así como en la aplicación y respecto de los derechos fundamentales, incrementando un mejor comercio electrónico con ayuda de tecnológica a través de las nuevas	Está claro que los delincuentes informáticos se mueven a pasos rápidos y se valen de que la normativa actual no refleja la realidad nacional. El vacío legal produce que los delincuentes actúen con impunidad.

	presencia en los casos del día a día eran casi nulos. Recién el año 2020, bajo el contexto de la Pandemia, surgió su comisión en gran escala, lo cual generó múltiples estudios, comentarios y recomendaciones al respecto. La normativa es clara y acorde a la realidad nacional, el detalle está en la operatividad tecnológica para identificar e individualizar a los presuntos autores o participes, tarea que, lamentablemente, no se puede realizar desde un despacho fiscal.	incorporaciones normativas; por tanto, el Estado debe brindar mayores capacitaciones a los operadores judiciales de acuerdo a la actual realidad informática, así como de las normas que sancionan las conductas fraudulentas.	

ANÁLISIS	Si, como bien se sabe a pesar de que la norma se encuentre establecida hace 8 años, aún existe nuevos medios tecnológicos que no se encuentran regulados en la legislación, pues incrementando un mejor control electrónico, se estaría brindando mayor capacitación a los operadores judiciales y la sanción de las normas ante las nuevas conductas fraudulentas.		
P2. OG2 ¿Qué se debería mejorar en la Ley de delitos informáticos?	Se debería añadir un par de párrafos o artículos, mediante los cuales se desarrolle una serie de técnicas sistemáticas recomendadas por ingenieros de sistemas que permitan facilitar la etapa preliminar de investigación, tanto al personal policial como trabajadoras del Ministerio Público.	Se debe de aplicar mejores mecanismos de ciberseguridad, ello con la finalidad de contar con un mayor control tecnológico, además, por parte del Estado se debería impartir capacitación y propagar campañas de alertas ante los nuevos delitos cibernéticos. Así mismo, sería de mucho aporte de que los legisladores promulguen normas acordes a las conductas no tipificadas aun; y así los	Se debe incorporar nuevos tipo penal que sancionen el accionar delictivo de los delincuentes informáticos de otro lado se debería facultar a los fiscales para acceder al levantamiento del secreto de las telecomunicaciones

		operadores jurídicos impongan correctamente las sanciones conforme a la gravedad de las nuevas modalidades de fraude informático.	
ANÁLISIS	Se debería incorporar nuevos artículos que involucren a un ingeniero de sistemas dentro de la investigación preliminar, así como al personal policial y al Ministerio Publico, esta modificación normativa tiene que ir en función a la ciberseguridad y a las conductas aun no tipificadas, facultando un mejor control tecnológico y fiscalizando el acceso al secreto de las comunicaciones.		
P3. OG2 ¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático?	Se debería realizar, mediante una coordinación interinstitucional entre el Ministerio Publico y la PNP, una serie de capacitaciones de carácter digital respecto a la forma y manejo de equipos sofisticados, programas y rutas a seguir con el soporte técnicos	Tanto el Ministerio Público, así como la Policía Nacional del Perú, deben contar con mejores herramientas de apoyo, ello a fin de poder identificar plenamente e individualizar a aquellas personas que haciendo uso de la tecnología cometen fraudes informáticos, es	Se debe estandarizar el desempeño de los efectivos policiales y los fiscales. Se debe protocolizar los plazos y las acciones de investigación para este tipo de casos.

	apropiado que deberían contar estas 2 instituciones, de esa manera se coadyuvaría el manejo para poder identificar e individualizar a los autores y participes con los elementos que el tipo penal exige.	más, se debe brindar mayor seguridad a las víctimas que resultan perjudicadas. Además, se debe tomar un mejor control y manejo de la información interna, esto es, proteger cuidadosamente los datos personales de la víctima, para contar con una mejor confiabilidad, integridad y disponibilidad. Finalmente, se debe sancionar merecidamente a las personas responsables e involucradas en los delitos informáticos con una pena equivalente a su conducta desplegada que ocasionó perjuicio a los agraviados.	

ANÁLISIS	Debería existir una previa coordinación con ambas entidades, así como tener las herramientas adecuada para poder identificar el uso de las tecnologías y fraude informático, finalmente se debe tomar en cuenta los plazos y las acciones de investigación ante este tipo de casos, generando una mejor confiabilidad, integridad y disponibilidad de los datos de la víctima.
CONCLUSIÓN	Tanto la falta de conocimiento como la falta de dominio dentro de la investigación se debe a que existe una mala aplicación normativa, ya que a pesar de la norma establecida aún no se presentan los nuevos medios tecnológicos, con el fin de incrementar un mejor control electrónico y una mayor capacitación jurídica a los operadores de justicia, asimismo se establece que la actual ley de delitos informáticos debería aplicar nuevos artículos que involucren una mejor ciberseguridad, pues las medidas aplicadas por el Ministerio Público y la Policía Nacional no son eficazmente relacionados con los delitos, es por eso que entre ambas entidades debe existir una mejor coordinación para brindar medidas adecuadas que ayuden a identificar el uso de las tecnologías y el fraude informático brindando una mejor confiabilidad, integridad y disponibilidad ante los datos de la víctima.

INSTRUMENTO DE RECOLECCIÓN DE DATOS ANEXO: 03

GUIA DE ENTREVISTA

DIRIGIDO A ABOGADOS, FISCALES PROVINCIALES Y ASISTENTES EN FUNCIÓN FISCAL.

Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021

ENTREVISTADO: ……...

CARGO: ……

INSTITUCIÓN: ……

OBJETIVO GENERAL

Determinar cuáles son las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

1. En su opinión, **¿Cuáles considera usted que son las deficiencias en las investigaciones fiscales por delitos de fraude informático en función a la Ley 30171?**

_____
_____
_____
_____

2. En referencia a la pregunta anterior, **¿Considera usted que estas deficiencias se deben a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?**

_____
_____
_____
_____

OBJETIVO ESPECIFICO 1

Analizar como la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

3. A su parecer, **¿A qué se debe la existencia de una deficiente investigación fiscal con relación a los delitos informáticos?**

_____
_____
_____
_____
_____
_____
_____

4. A su criterio, **¿La deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática?**

_____
_____
_____
_____
_____
_____
_____

5. Para usted, **¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático?**

_____
_____
_____
_____
_____
_____
_____

OBJETIVO ESPECIFICO 2

Analizar como la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

6. En su opinión, **¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático se debe a que la normativa no está acorde a la realidad nacional?**

_____
_____
_____
_____
_____
_____

7. De su respuesta anterior, **¿Qué se debería mejorar en la Ley de delitos informáticos?**

_____
_____
_____
_____
_____

8. En conclusión, **¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático?**

_____
_____
_____
_____
_____

INSTRUMENTO DE RECOLECCIÓN DE DATOS ANEXO: 02

GUIA DE ENTREVISTA

DIRIGIDO A ABOGADOS, FISCALES PROVINCIALES Y ASISTENTES EN FUNCIÓN FISCAL.

Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021

ENTREVISTADO: Haddad Juseff Chaname Vasquez

CARGO: Abogado

INSTITUCIÓN: Independiente – Distrito Fiscal de Lima

OBJETIVO GENERAL

Determinar cuáles son las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

1. En su opinión, **¿Cuáles considera usted que son las deficiencias en las investigaciones fiscales por delitos de fraude informático en función a la Ley 30171?**

   Las deficiencias que se advierten en las investigaciones fiscales son: la falta de Capacitación a los órganos jurisdiccionales, mala aplicación de la norma; vacíos legales, criminalidad tecnológica, falta de dominio de investigación.

2. En referencia a la pregunta anterior **¿Considera usted que estas deficiencias se deben a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?**

Se debe a ambas, debido a que por una parte la norma no regula correctamente los nuevos delitos cibernéticos, ni mucho menos toma en cuenta el avance tecnológico y por otra los órganos judiciales no están debidamente capacitados por el Estado, ante los nuevos casos de fraude informático.

OBJETIVO ESPECIFICO 1

Analizar como la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

3. A su parecer, **¿A qué se debe la existencia de una deficiente investigación fiscal con relación a los delitos informáticos?**

Se debe a que las investigaciones no tienen valor normativo ni judicial, debido a que los nuevos alcances de modalidad de fraude tecnológico no se encuentran actualizados en la norma, ni en la capacitación de los juzgadores.

4. A su criterio, **¿La deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática?**

Si, ya que los nuevos medios de fraude tecnológico aún no se encuentran regulados en la norma, y por lo tanto no tiene una pena establecida que ayude a poder contrarrestar estos nuevos delitos en función a la criminalidad informática.

5. Para usted, **¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático?**

Primero, se debe actualizar la norma, a la realidad social, incorporando las diversas modalidades habidas y por haber; segundo, debería implementarse capacitaciones a los servidores y funcionarios públicos del Ministerio Publico y la Policía Nacional del Perú, a fin de aplicar la ciberseguridad y un control de confidencialidad de la información.

OBJETIVO ESPECIFICO 2

Analizar como la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

6. En su opinión, **¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático se debe a que la normativa no está acorde a la realidad nacional?**

Si, para ello se tiene que basar en las nuevas tecnológicas y en los derechos fundamentales, incrementando un mejor comercio electrónico, a través de las

nuevas incorporaciones normativas y capacitando a los operadores judiciales de acuerdo a la actual realidad informática.

7. De su respuesta anterior, **¿Qué se debería mejorar en la Ley de delitos informáticos?**

   - Se debería implementar mejores mecanismos de ciberseguridad
   - Se debería aplicar un control tecnológico
   - Se debería impartir una capacitación ante los nuevos delitos cibernéticos
   - Y se debería ejecutar nuevas penas conforme a la gravedad de las nuevas modalidades de fraude informático.

8. En conclusión, **¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático?**

   - Mejores medios de identificación de fraude cibernético
   - Seguridad a las victimas
   - Mejorar la confiabilidad, integridad y disponibilidad
   - Mejorar el manejo de la información interna
   - Responsabilidad penal a las personas involucradas en los delitos cibernéticos

INSTRUMENTO DE RECOLECCIÓN DE DATOS ANEXO: 02

GUIA DE ENTREVISTA

DIRIGIDO A ABOGADOS, FISCALES PROVINCIALES Y ASISTENTES EN FUNCIÓN FISCAL.

Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021

ENTREVISTADO : JEFFERSON RIVERO GUISADO

CARGO : ASISTENTE DE FUNCIÓN FISCAL

INSTITUCIÓN : 20° FISCALIA PROVINCIAL PENAL DE LIMA

OBJETIVO GENERAL
Determinar las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

1. En su opinión, **¿Cuáles considera usted que son las deficiencias en las investigaciones fiscales por delitos de fraude informático en función a la Ley 30171?**

   Considero que las deficiencias en las investigaciones fiscales por los delitos de fraude informático, se debe principalmente a la falta de capacitación tanto a los funcionarios y servidores públicos de los órganos jurisdiccionales; lo que causa una falta de dominio de investigación y una mala aplicación de la norma en perjuicio del bien jurídico protegido ; sumado a ello, se debe tener en cuenta los vacíos legales que existen y que no protegen ciertas conductas en cuanto a la criminalidad tecnológica que cada día es más frecuente.

2. En referencia a la pregunta anterior, **¿Considera usted que estas deficiencias se deben a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?**

   En mi opinión, considero que se debe a ambas, debido a que por una parte, al existir ciertos vacíos legales, la norma no regula correctamente los nuevos delitos cibernéticos que a la fecha se han incrementado, ni mucho menos toma en cuenta el avance tecnológico; por otra parte, el personal de los órganos judiciales no están debidamente capacitados por el Estado a efectos de poder conducir una adecuada y correcta investigación ante los nuevos casos de fraude informático del cual muchas personas son víctimas de estos delitos.

OBJETIVO ESPECIFICO 1

Analizar si la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

3. A su parecer, **¿A qué se debe la existencia de una deficiente investigación fiscal con relación a los delitos informáticos?**

   Esto se debe a que las investigaciones preliminares no tienen valor normativo ni judicial, debido a que los nuevos alcances de modalidad de fraude tecnológico no se encuentran actualizados en la norma, ni en la capacitación de los juzgadores, es más, tanto la Fiscalía como la Policía Nacional del Perú no siempre cuentan con las herramientas suficientes a fin de poder identificar e individualizar al autor o autores de los delitos informáticos.

4. A su criterio, **¿La deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática?**

   Considero de que sí, dado que los nuevos medios de fraude tecnológico en su totalidad, aún no se encuentran regulados en la norma penal, por consiguiente dichas conductas no tienen una pena establecida que coadyuve a poder contrarrestar estos nuevos delitos en función a la criminalidad informática, así como poder sancionar a los autores del mismo.

5. Para usted, **¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático?**

   Definitivamente se debe capacitar a los funcionarios y servidores de los órganos jurisdiccionales, ello a efectos de que puedan tener un mejor panorama jurídico en cuanto a los delitos informáticos; asimismo, tanto los legisladores como los magistrados deben de actualizar así como analizar a mayor profundidad la norma aplicable a los delitos informáticos.

   Aunado a ello, el Estado debe brindar programas de orientación a la ciudadanía, y estos puedan aplicar la ciber seguridad a efectos de no resultar perjudicados y poder llevar un mejor control de confidencialidad.

OBJETIVO ESPECIFICO 2

Analizar si la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

6. En su opinión, **¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático se debe a que la normativa no está acorde a la realidad nacional?**

   Opino que sí, pues para ello se tiene que basar en las nuevas herramientas tecnológicas así como en la aplicación y respeto de los derechos fundamentales, incrementando un mejor comercio electrónico con ayuda de la tecnología a través de las nuevas incorporaciones normativas; por tanto, el Estado debe brindar mayor capacitaciones a los operadores judiciales de acuerdo a la actual realidad informática, así como de las normas que sancionan las conductas fraudulentas.

7. De su respuesta anterior, **¿Qué se debería mejorar en la Ley de delitos informáticos?**

   Considero que principalmente se debe implementar mejores mecanismos de ciber seguridad, ello con la finalidad de contar con un mayor control tecnológico, además, por parte del Estado se debería impartir capacitación y propagar campañas de alertas ante los nuevos delitos cibernéticos. Asimismo, seria de mucho aporte de que los legisladores promulguen normas acordes a las conductas no tipificadas aun; y así los operadores jurídicos impongan correctamente las sanciones conforme a la gravedad de las nuevas modalidad de fraude informático.

8. En conclusión, **¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático?**

   Tanto el Ministerio Público así como la Policía Nacional del Perú, deben contar con mejores herramientas de apoyo, ello a fin de poder identificar plenamente e individualizar a aquellas personas que haciendo uso de la tecnología cometen fraudes informáticos, es más, se debe brindar mayor seguridad a las víctimas que resultan perjudicadas.

   Además, se debe tomar un mejor control y manejo de la información interna, esto es, proteger cuidadosamente los datos personales de la víctima, para contar con una mejor confiabilidad, integridad y disponibilidad.

   Finalmente, se debe sancionar merecidamente a las personas responsables e involucradas en los delitos informáticos con una pena equivalente a su conducta desplegada que ocasionó perjuicio a los agraviados.

Jefferson Rivero Guisado
Asistente en Función Fiscal
20° FPP-L

INSTRUMENTO DE RECOLECCIÓN DE DATOS ANEXO: 02

GUIA DE ENTREVISTA

DIRIGIDO A ABOGADOS, FISCALES Y ASISTENTES EN FUNCIÓN FISCAL.

Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021

ENTREVISTADO: Jhean Franco Cifuentes Dávila

CARGO: Fiscal Adjunto Provincial Penal Titular de Lima

INSTITUCIÓN: Ministerio Público

OBJETIVO GENERAL
Determinar las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

1. En su opinión, **¿Cuáles considera usted que son las deficiencias en las investigaciones fiscales por delitos de fraude informático en función a la Ley 30171?**

En mis años de experiencia, tanto de asistente en función fiscal como de magistrado, me pude percatar que el problema fundamental radica en la muy difícil capacidad para lograr identificar objetivamente a los presuntos autores de estos delitos y, a su vez, vincularlos con los elementos típicos para la consumación con el tipo penal.

2. En referencia a la pregunta anterior, **¿Considera usted que estas deficiencias se deben a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?**

Se debe, en mi opinión, a la falta de capacitación por parte del Estado a los órganos "policiales", mas no a los judiciales. Hago esa precisión puesto que, los juzgados no "investigan", sino el Ministerio Público en directa coordinación con la PNP especializada para esta clase de delitos.

OBJETIVO ESPECIFICO 1
Analizar si la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

3. A su parecer, **¿A qué se debe la existencia de una deficiente investigación fiscal con relación a los delitos informáticos?**

La deficiencia en las investigaciones fiscales respecto a los delitos informáticos obedece básicamente a la falta de operatividad por parte de la Unidad de Investigación que se avoca a los delitos de Alta Tecnología (DIVINDAT), ya que estos casos no se pueden llevar a cabo en "sede fiscal", dado que, en un despacho no se cuenta con equipos sofisticados para ello, sino todo lo contrario.

4. A su criterio, **¿La deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática?**

No considero que existan vacíos legales para el tipo penal de Fraude Informático, ya que la Ley Especial con la cual se incorporó este delito y otros de naturaleza similar, desarrollan correctamente el alcance de sus verbos rectores; sin embargo, sí considero que existe una escasez de normativa

5. Para usted, **¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático?**

El Estado peruano debería brindar mayor implementación de equipos tecnológicos a la vanguardia del Siglo XXI, los cuales permitirían una mejor investigación respecto a la naturaleza de este delito.

OBJETIVO ESPECIFICO 2
Analizar si la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

6. En su opinión, **¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático se debe a que la normativa no está acorde a la realidad nacional?**

Si bien es cierto, los delitos informáticos en general (no específicamente el "fraude informático") se encuentran regulados hace aproximadamente 08 años atrás, resulta que desde ese entonces era de carácter simbólico en el Código Penal, ya que su presencia en los casos del día a día eran casi nulos. Recién el año 2020, bajo el contexto de la Pandemia, surgió su comisión en gran escala, lo cual generó múltiples estudios, comentarios y recomendaciones al respecto. La normativa es clara y acorde a la realidad nacional, el detalle está en la operatividad tecnológica para identificar e individualizar a los presuntos autores o partícipes, tarea que, lamentablemente, no se puede realizar desde un despacho fiscal.

7. De su respuesta anterior, **¿Qué se debería mejorar en la Ley de delitos informáticos?**

Se debería añadir un par de párrafos o artículos, mediante los cuales se desarrolle una serie de técnicas sistemáticas recomendadas por ingenieros de sistemas que permitan facilitar la etapa preliminar de investigación, tanto al personal policial como trabajadores del Ministerio Público.

8. En conclusión, **¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático?**

Se debería realizar, mediante una coordinación interinstitucional entre el Ministerio Público y la PNP, una serie de capacitaciones de carácter digital respecto a la forma y manejo de equipos sofisticados, programas y rutas a seguir con el soporte técnico apropiado que deberían contar estas 2 instituciones, de esa manera se coadyuvaría el manejo para poder identificar e individualizar a los autores y partícipes con los elementos que el tipo penal exige.

Jhean Franco Cifuentes Dávila
Fiscal Adjunto Provincial (T)
Distrito Fiscal de Lima

INSTRUMENTO DE RECOLECCIÓN DE DATOS ANEXO: 02

GUIA DE ENTREVISTA

DIRIGIDO A ABOGADOS, FISCALES PROVINCIALES Y ASISTENTES EN FUNCIÓN FISCAL.

Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021

ENTREVISTADO: CLARITA JUDITH FLORES BORJA

CARGO: FISCAL ADJUNTO PROVINCIAL

INSTITUCIÓN: MINISTERIO PÚBLICO – FISCALIA DE LA NACIÓN

OBJETIVO GENERAL
Determinar las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

1. En su opinión, **¿Cuáles considera usted que son las deficiencias en las investigaciones fiscales por delitos de fraude informático en función a la Ley 30171?**

Considero que una de las deficiencias en el desarrollo de las investigaciones por estos delitos es la falta de capacitación del personal fiscal, tenemos también la excesiva carga presente en este último periodo, y un escaso apoyo por parte de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), quienes pese a ser una unidad especializada no mantienen en primer plano una directa coordinación con el Despacho Fiscal en el manejo de estos casos, generando en su mayoría que recaigan en archivo por no lograr acopiar elementos objetivos que logren identificar al autor o enervar la presunción de inocencia de los presuntos implicados.

2. En referencia a la pregunta anterior, **¿Considera usted que estas deficiencias se deben a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?**

Se aprecia ambos casos, ello a razón que la norma no se encuentra regulada acorde a las nuevas modalidades que han manifestado últimamente, los mismos que claramente requieren una constante capacitación por parte del Ministerio Publico para una investigación más objetiva.

OBJETIVO ESPECIFICO 1

Analizar si la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

3. A su parecer, **¿A qué se debe la existencia de una deficiente investigación fiscal con relación a los delitos informáticos?**

La complejidad que contienen los delitos informáticos requiere necesariamente que estos sean ventilados ante una unidad especializada, en este caso la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), ahora bien, al hablar de deficiencias hacemos mención a que resulta insostenible la posibilidad de llevar a cabo la investigación a nivel fiscal por cuanto no se cuenta con los equipos tecnológicos necesarios; sin embargo, el problema radica que también tenemos como déficit la falta de operatividad por parte de la unidad especializada.

4. A su criterio, **¿La deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática?**

Considero que no se aprecia vacíos legales en la Ley Especial sobre el delito de fraude informático, lo que si se tiene presente es una escasa normativa ante la comisión de estos casos sin mediar que actualmente han ido brotando nuevas modalidades que deben ser incorporados.

5. Para usted, **¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático?**

Debe implementar mesas de trabajo entre la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) y el Ministerio Público a fin de establecer criterios de investigación objetivos, asimismo, se debe brindar mayor implementación de equipo tecnológico de alta gama para la naturaleza de este delito.

OBJETIVO ESPECIFICO 2

Analizar si la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

6. En su opinión, **¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático se debe a que la normativa no está acorde a la realidad nacional?**

La normativa es clara en cuestión a estos delitos, sin embargo, surge la necesidad de una adecuada operatividad en la tecnológica que coadyuve en la identificación e individualización de los presuntos implicados.

7. De su respuesta anterior, **¿Qué se debería mejorar en la Ley de delitos informáticos?**

Se debería incorporar párrafos donde consideren una serie de técnicas sistemáticas en merito a los aportes brindados por los ingenieros de sistemas, a fin de viabilizar la investigación a nivel preliminar.

8. En conclusión, **¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático?**

Las medidas que deberían implementarse son un plan de acción interinstitucional entre la Fiscalía y la PNP, los cuales permitirían exponer y capacitar al personal a cargo de estos casos sobre materia digital a fin de establecer un protocolo de trabajo unificado en aras de identificar e individualizar a los autores y participes con los elementos idóneos requeridos por ley.

CLARITA JUDITH FLORES BORJA
Fiscal Adjunto Provincial
1° Despacho - 1° Fiscalía Penal Corporativa de
Lima Centro - Rimac - Breña - Jesús María

INSTRUMENTO DE RECOLECCIÓN DE DATOS ANEXO: 02

GUIA DE ENTREVISTA

DIRIGIDO A FISCALES SUPERIORES, FISCALES PROVINCIALES Y ASISTENTES EN FUNCIÓN FISCAL.

Deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima - 2021

ENTREVISTADO: JESUS VICTOR HUAMAN ORTEGA

CARGO: ABOGADO

INSTITUCIÓN: .....

OBJETIVO GENERAL
Determinar las deficiencias en las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

1. En su opinión, **¿Cuáles considera usted que son las deficiencias en las investigaciones fiscales por delitos de fraude informático en función a la Ley 30171?**

Considero que existe deficiencias en las investigaciones por falta de capacitación de los diferentes sujetos procesales como la policia, el ministerio publico y los jueces, toda vez que estos delitos tratan sobre tecnologias nuevas por lo que se requiere una constante capacitación ademas de una legislación acorde.

2. En referencia a la pregunta anterior, **¿Considera usted que estas deficiencias se deben a la mala aplicación de la norma o a la falta de capacitación por parte del Estado a los órganos judiciales?**

Ademas de la falta de capacitación, existe una falta de personal especializado en la policía y ministerio publico, que puedan resolver estos casos con la celeridad que se requiere.

OBJETIVO ESPECIFICO 1

Analizar si la deficiente investigación fiscal perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

3. A su parecer, **¿A qué se debe la existencia de una deficiente investigación fiscal con relación a los delitos informáticos?**

DEBEMOS CONSIDERAR QUE LA POLICIA NACIONAL Y EL MINISTERIO PUBLICO PRESENTA UNA ALTA CARGA PROCESAL EN DELITOS CONTRA EL PATRIMONIO, ADEMAS LA FALTA DE PERSONAL ESPECIALIZADO HACE QUE LAS INVESTIGACIONES EN DELITOS INFORMATICOS SEAN DEFICIENTES.

4. A su criterio, **¿La deficiente investigación fiscal se debe a los diferentes vacíos legales y escasez de normativa en relación a la criminalidad informática?**

LOS DELINCUENTES INFORMATICOS HACEN USO DE TECNOLOGIAS NOVEDOSAS POR LO QUE ES NECESARIO UNA LEGISLACION ACORDE A ESTA REALIDAD. SI BIEN TENEMOS LA LEY 30171, ESTA LEGISLACIÓN NO RECOGE TODAS LAS ACTUALES MODALIDADES DE FRAUDE INFORMATICO, POR LO QUE EL ESTADO DEBERÍA INCORPORAR NUEVOS TIPOS PENALES.

5. Para usted, **¿Qué medidas debe implementar el Estado peruano para poder resolver mejor los casos de fraude informático?**

PRIMERO, SE DEBE ESTABLECER PROTOCOLOS DE ACCIÓN INMEDIATA QUE PERMITAN IDENTIFICAR DE MANERA RAPIDA A LOS DELINCUENTES INFORMATICOS. LA POLICIA DEBE CONTAR CON HERRAMIENTAS TECNOLOGICAS PARA IDENTIFICAR LOS IP AL BIEN RECIBA LA DENUNCIA.

OBJETIVO ESPECIFICO 2

Analizar si la falta de conocimiento y dominio perjudica las investigaciones por delitos de fraude informático en el distrito fiscal de Lima – 2021

6. En su opinión, **¿La falta de conocimiento y dominio en las investigaciones por delitos de fraude informático se debe a que la normativa no está acorde a la realidad nacional?**

ESTA CLARO QUE LOS DELINCUENTES INFORMATICOS SE MUEVEN A PASOS MAS RÁPIDOS Y SE VALEN DE QUE LA NORMATIVA ACTUAL NO REFLEJA LA REALIDAD NACIONAL. EL VACIO LEGAL PRODUCE QUE LOS DELINCUENTES ACTUEN CON IMPUNIDAD.

7. De su respuesta anterior, **¿Qué se debería mejorar en la Ley de delitos informáticos?**

SE DEBE INCORPORAR NUEVOS TIPOS PENAL QUE SANCIONEN EL ACCIONAR DELICTIVO DE LOS DELINCUENTES INFORMATICOS. DE OTRO LADO SE DEBERÍA FACULTAR A LOS FISCALES PARA ACCEDER AL LEVANTAMIENTO DEL SECRETO DE LAS TELECOMUNICACIONES.

8. En conclusión, **¿Qué medidas debe tomar el Ministerio Publico y la Policía Nacional para aplicar correctamente la norma penal en relación a los delitos de fraude informático?**

SE DEBE ESTANDARIZAR EL DESEMPEÑO DE LOS EFECTIVOS POLICIALES Y LOS FISCALES. SE DEBE PROTOCOLIZAR LOS PLAZOS Y LAS ACCIONES DE INVESTIGACION PARA ESTE TIPO DE CASOS.

CAL Nº 83455

UNIVERSIDAD CÉSAR VALLEJO

ESCUELA DE POSGRADO

MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL

Declaratoria de Originalidad del Autor

Yo, IVEETT DEL ROSARIO CARRERA PEÑA estudiante de la ESCUELA DE POSGRADO MAESTRÍA EN DERECHO PENAL Y PROCESAL PENAL de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Declaratoria de Originalidad del Autor / Autores titulada: "DEFICIENCIAS EN LAS INVESTIGACIONES POR DELITOS DE FRAUDE INFORMÁTICO EN EL DISTRITO FISCAL DE LIMA - 2021", es de mi autoría, por lo tanto, declaro que la Declaratoria de Originalidad del Autor / Autores:

1. No ha sido plagiada ni total, ni parcialmente.
2. He mencionado todas las fuentes empleadas, identificando correctamente toda cita textual o de paráfrasis proveniente de otras fuentes.
3. No ha sido publicada ni presentada anteriormente para la obtención de otro grado académico o título profesional.
4. Los datos presentados en los resultados no han sido falseados, ni duplicados, ni copiados.

En tal sentido asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

Nombres y Apellidos	Firma
IVEETT DEL ROSARIO CARRERA PEÑA **DNI:** 71498082 **ORCID:** 0000-0003-4071-6241	Firmado digitalmente por : ICARRERAP el 07-08-2021 22:12:29

Código documento Trilce: TRI - 0176365

INVESTIGA UCV