FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-comerce.* 2021

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE

Abogado

AUTOR:

VERASTEGUI QUINTANILLA, Cesar Jonathan (ORCID: 0000-0002-6629-7770)

ASESORES:

Mg. Chávez Suárez, Giancarlo Renan (ORCID: 0000-0001-8053-6136)

Mg. Guerra Campos, Jefferson Williams (ORCID: 0000-0003-0158-7248)

LÍNEA DE INVESTIGACIÓN:

Derecho Penal

LIMA - PERÚ

2022

Dedicatoria

A mi familia conyugal (Mi esposa Verónica, mi Hijo Jonathan Omar y mi Hija Aamara Catalina) por ser la fuente principal de inspiración y desarrollo en todos los proyectos realizados, anhelando ser la senda para sus proyectos de vida.

Agradecimiento

A los docentes que coadyuvaron en mi formación profesional y a mi familia por todo el respaldo brindado en todos estos años de dedicación académica.

Índice de contenidos

Índice de tablas

Índice de figuras

Resumen

El estudio titulado El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-comerce.* 2021, tuvo por objetivo determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-comerce* en la lucha contra la ciberdelincuencia en el periodo 2021. Para ello se aplicó un enfoque cualitativo con técnicas de análisis de fuente documental y entrevista a expertos, desde un tipo de estudio básico y de diseño de teoría fundamentada. Los instrumentos fueron debidamente validados y se contó con el rigor científico de los mismos.

Al final del estudio se concluye que el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-comerce,* resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021. Es por ello que se plantean una serie de recomendaciones viables y factibles a fin de que tanto la Oficina Técnica del Ministerio Público de Lima centro como la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional, fortalezcan sus acciones y estrategias para combatir este delito que cada vez se expande más en el país y en el mundo.

***Palabras clave*:** *E-comerce,* delito de fraude informático, rol del Ministerio Público de Lima centro, División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional.

Abstract

The study entitled El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del E-comerce. 2021, aimed to determine the role of the Public Prosecutor's Office of central Lima in the prosecution of the crime of computer fraud committed through E-comerce in the fight against cybercrime in the period 2021. For this purpose, a qualitative approach was applied with techniques of documentary source analysis and expert interview, from a basic study type and grounded theory design. The instruments were duly validated and their scientific rigor was ensured.

At the end of the study, it is concluded that the role of the Public Prosecutor's Office of central Lima in the prosecution of the crime of computer fraud committed through E-comerce was not very significant since it did not have the infrastructure, logistics and suitable personnel to fight against cybercrime in the period 2021. For this reason, a series of viable and feasible recommendations are put forward so that both the Technical Office of the Public Prosecutor's Office in central Lima and the High Technology Crime Investigations Division of the National Police can strengthen their actions and strategies to combat this crime that is increasingly expanding in the country and the world.

Key words: E-comerce, computer fraud, role of the Public Prosecutor's Office of central Lima, High Technology Crime Investigations Division of the National Police.

I. INTRODUCCIÓN

El interés por analizar y evaluar el rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-comerce*, surge de la realidad problemática planteada por los criminólogos cuando señalaban que un delito sucede cuando se juntan cuatro aspectos: una norma, un causante, un propósito y un lugar. Sin embargo, con el uso de la internet y de la tecnología de la información y comunicación, los especialistas han empezado a analizar que la definición del delito debe revisarse ya que estos ilícitos se cometen en "no lugares". Estas modificaciones han aperturado diferentes líneas de estudio (Elías, 2014). En ese sentido, desde el presente trabajo se aborda la problemática que ha generado el fraude informático y todas sus implicancias legales, sociales y económicas.

Ya desde el año 1994 durante el XV Congreso Internacional de Derecho Penal, señalaba que la academia en conjunto con los Estados debe unir esfuerzos para desarrollar más estudios sobre el delito cometidos a través del uso de la informática. El Derecho debe considerar el análisis y desarrollo de la norma, considerando las cualidades propias de la data, al asemejarla con los elementos verificables y analizar las posibles modificaciones que vulneran los bienes jurídicos.

Desde ese año hasta la actualidad, el Perú ha avanzado de manera poco significativa en relación a implementar una política criminal que combata el ciberdelito, el fraude informático, el *E-comerce,* y delitos cometidos a través de plataformas tecnológicas. Así, se cuenta con la tipificación del delito de hurto telemático regulado en el artículo 186 del Código Penal, castigándolo con pena privativa de libertad no menor de tres ni mayor de seis años y con 180 a 365 días-multa, cuando el delincuente utilizaba medios de transferencia virtual de dinero, de la informática o alteraba el uso de claves ocultas. Asimismo, se aprobó la Ley N°. 26319 del 27 de mayo de 1994, la misma que incrementó la sanción a una pena no menor de cuatro ni mayor de ocho años, continuando sin cambios significativos hasta que fue modificada por Ley 30096 del 27 de septiembre de 2013. Ante ello, el legislador consideró que este tipo penal sólo sancionaba pocas conductas ilícitas y dejaba libres otros delitos en los que se usaban medios tecnológicos.

Por lo expuesto, con el presente estudio se quiere presentar el diagnóstico de la situación, las limitaciones, dificultades, así como los desafíos que el Estado debe enfrentar para abordar de modo decidido el ciberdelito, el fraude informático, el *E-comerce,* y los delitos cometidos a través de plataformas tecnológicas. Pues creemos, al igual que Elías que se requieren renovar los medios de comunicación con las instancias políticas para aumentar la experiencia en la lucha contra este nuevo delito global y eludir que las modificaciones legales se hagan sin conocimiento público y sin contar con la ciudadanía. Del mismo modo, se requiere compartir este intercambio con los expertos y la población pues son ellos quienes están expuestos a estos ilícitos y serán ellos quienes los denuncien ante las instancias respectivas para aclarar lo sucedido. Este reto es arduo, pero se requiere tomar decisiones para ejercer los derechos plenamente y exhortar que se respeten las garantías.

Por lo tanto, se plantearon los siguientes problemas de investigación. Problema General: ¿Cuál fue el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-comerce* en la lucha contra la ciberdelincuencia en el periodo 2021?, como problema específico 1: ¿Cuál fue el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021?, y como problema específico 2: ¿Cuál fue la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021?

El estudio se justifica desde los siguientes aspectos: Justificación práctica. La investigación se justifica en la práctica por la necesidad de analizar el rol del Ministerio Público de Lima centro y la Policía Nacional en el cumplimiento de la Ley N° 30096 que sanciona el fraude informático cometido a través del E-comerce en la lucha contra la ciberdelincuencia, desde luego se podrá propiciar una discusión jurídica, socioeconómica y de distintos aspectos en relación al estudiado con ocasión de la investigación que nos convoca desarrollar, luego del cual se plantean

recomendaciones con el propósito de enfrentar el delito de fraude informático que tanto perjudica a la sociedad.

Respecto a la justificación teórica. Este estudio se justificó en lo teórico ya que tiene el respaldo de los principales expertos en la materia. Además, se utilizó un marco teórico especializado. Recientemente el fraude informático, el E-comerce y la ciberdelincuencia han sido desarrollados en todo el mundo de modo recurrente y por eso mismo requiere mayores estudios pues se trata de un delito dinámico y cambiante. Cabe señalar que el fraude informático y la ciberdelincuencia se ha expandido en estos últimos años, más todavía en un contexto de pandemia, la cual no ha tenido un tratamiento idóneo en la legislación nacional, estando la sociedad desprotegida por el Estado, es por ello que esta investigación se justifica porque buscó establecer criterios teóricos según las circunstancias para lograr una adecuada estrategia criminal y penal para contrarrestar los efectos perniciosos del fraude informático y la ciberdelincuencia.

Justificación metodológica. El estudio asumió criterios de investigación y técnicas de recojo de información, ello con el fin de analizar los diversos factores influyentes en el fraude informático y la ciberdelincuencia, como el perfil socioeconómico de los delincuentes y las víctimas, así como también el rol del Estado, a través del Ministerio Público (MP) y la Policía Nacional del Perú (PNP), en torno a este delito.

De igual modo, se plantearon los siguientes objetivos de investigación. Objetivo General: Determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-comerce* en la lucha contra la ciberdelincuencia en el periodo 2021, como objetivo específico 1: Evaluar el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021, y como objetivo específico 2: Evaluar la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021.

Así entonces se plantean las siguientes hipótesis. Hipótesis General: El rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-comerce,* resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021, como Hipótesis Específicas 1: El rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó limitado ya que no contó con implementos tecnológicos y logística especializada que le permita llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos en el periodo 2021 y como Hipótesis Específica 2: La labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó deficiente ya que no contó con personal calificado, logística, infraestructura, recursos, capacitación y actualización permanente para que el personal lleve a cabo operativos de prevención e intervención en estos delitos en el periodo 2021.

II. MARCO TEÓRICO

Antecedente internacional. El estudio de Price Wáter House Cooper (2014) titulado *Global Economic Survey,* tuvo por objetivo realizar una encuesta económica a nivel mundial para precisar la incidencia del ciberdelito, desde un enfoque cuantitativo obtiene por resultado que este delito está cada vez más en expansión y los Estados deben asumir medidas más efectivas para enfrentarla. El estudio concluye que la opinión sobre este tipo de delitos ha aumentado del 39% (2011) al 48% (2014) en todo el mundo. Es más, los ilícitos informáticos implican uno de los cinco fraudes más utilizados en el mundo empresarial (24%). Este estudio aportó en el conocimiento de los fraudes informáticos que se cometen en el ámbito empresarial.

El estudio de Asturias Corporación Universitaria (2018) titulada *Introducción al e-comerce*, tuvo por objetivo plantear los alcances conceptuales y teóricos sobre el e-comerce, desde un tipo de estudio cualitativo, obtiene como resultado que se trata de una figura jurídica con categorías, características y tipologías propias. En ella se concluye que cuando se habla de *E-comerce*, se refiere a una denominación que implica todos los aspectos comerciales en los que participe en algún momento cierto procedimiento electrónico, si bien actualmente la denominación se usa en un sentido más específico para señalar los procesos en los que se usa la internet para intercambiar las diferentes partes. El *E-comerce* ha evolucionado sobremanera en los últimos años, tanto que ha consolidado diferentes tipos de negocio, según los participantes: empresas, consumidores y Estado. Este estudio nos ayudó a comprender que el comercio electrónico para todo negocio supone ciertos beneficios (facilidad para la mundialización, el ahorro en costos o el inicio de un novedoso sistema de negocios) así como ciertos perjuicios que pueden limitar su auge.

De Argentina se cuenta con el estudio de Iglesias (2018) el cual tuvo por objetivo plantear estrategias para el manejo adecuado del comercio electrónico a fin de evitar estafas y fraudes. Se trató de un tipo de estudio cuantitativo. La autora obtiene como resultado que cada vez son más los peligros y riesgos al hacer uso

de los medios de comunicación digitalizada y por eso mismo se requiere mayor cuidado en su uso. La autora concluye que para aquellos que poseen comercio electrónico deben reconocer a su público a que utilicen de modo adecuado las redes sociales, sin dejar de lado el adecuado servicio y un trato humano durante todo el intercambio. El estudio aportó en la comprensión de que en la medida en que el emprendimiento aumente entonces deja de tercerizar servicios, por ejemplo, la logística para aumentar el valor y trato directo al usuario.

El estudio de Urbano (2017) titulado *Ventajas y desventajas del comercio electrónico*, tuvo por objetivo precisar los riesgos y posibilidades del uso del comercio electrónico ya que se trata de una práctica cada vez más común. El estudio fue de tipo cuantitativo, el autor obtiene como resultado que el mundo actual debe aprovechar las enormes ventajas que trae el comercio de forma digitalizada, tiene medidas de seguridad que se deben conocer y aplicar. El autor concluye que existen limitaciones para el acceso de las pequeñas empresas al comercio electrónico: 1) La seguridad: el fraude de pago de comercio electrónico y el cuidado de la data; 2) La competencia: las empresas del comercio electrónico; 3) Desconocido valor económico por medio del marketing; 4) No tener conocimiento y no contar con el personal calificado para plantearse el nuevo reto; 5) La retención de los usuarios, el cual se puede abordar con marketing, ofreciendo un óptimo servicio.

El estudio de Gutiérrez (2018) titulado *La razón del éxito del E-comerce*, de tipo cuantitativo, concluye que, para un importante número de personas, el comercio electrónico supone desconfianza, por lo que los negocios deben brindar confianza al consumidor, obligando a que toda su data íntima sea bien resguardada en su empresa. Además, señala que se requiere ofrecer una opción de precios favorables, que se resalten dentro de la competencia. El autor nos ayudó a comprender lo necesario de brindar, en el e-comerce, productos idóneos con propuestas de compra más adecuados y que cumplan con las demandas de los usuarios.

Antecedente nacional. El estudio de Mengoa (2021) tuvo por objetivo precisar los alcances de los delitos informáticos y analizar su tratamiento legal. Fue un estudio cualitativo y obtuvo como resultado que aún no se cuenta con una regulación eficaz para combatir este delito. El autor concluye que el *phishermule* no es un tipo establecido con precisión en la normativa de los delitos informáticos a pesar que vulneran los bienes de las personas. Asimismo, la autora señaló que el *phisher-mule* no está identificada para su tipificación en el Código Penal, por lo que se requiere elaborar una investigación más exhaustiva para su adecuada regulación en la norma. Este estudio aportó un análisis más técnico de la problemática del presente estudio.

El estudio de Espinoza (2017) tuvo por objetivo analizar el tratamiento operativo de los delitos informáticos y los vacíos y deficiencias encontradas. El estudio de enfoque cualitativo, obtuvo como resultado que el contexto actual obliga a contar con una legislación más efectiva que permita sancionar los delitos informáticos. El autor concluye que para prevenir estos delitos y fortalecer el poder de vigilancia, se debe considerar lo siguiente: a) cuidar la data que se publica en redes sociales, b) evitar difundir imágenes comprometedoras, c) No usar webcam con personas desconocidas, d) No atender mensajes que requieren datos personales, e) No hacer click en links, ni descargar data adjunta de mensajes que no se conocen.

El estudio de Morales (2016) tuvo por objetivo analizar el modo en que las autoridades aplican la normativa sobre delitos informáticos, el estudio de enfoque mixto, obtuvo como resultado que el operador de justicia debe ser capacitado para el manejo idóneo de las tecnologías de la información y comunicación. El autor concluye que con el resguardo de los derechos en las normas de los ilícitos informáticos se han ubicado otras normas con las que pudieran existir ciertas incoherencias para su mala aplicación; como por ejemplo el hurto y sus agravantes, que está regulado en el Código Penal. Actualmente, la delincuencia ha aumentado de modo considerable en el mundo y con la utilización de modos más sofisticados para llevar a cabo sus delitos como el uso de medios tecnológicos, siendo el arma

más pertinente para mitigar este ilícito es la aprobación de normas acordes con ese delito, tanto a nivel nacional, local y mundial.

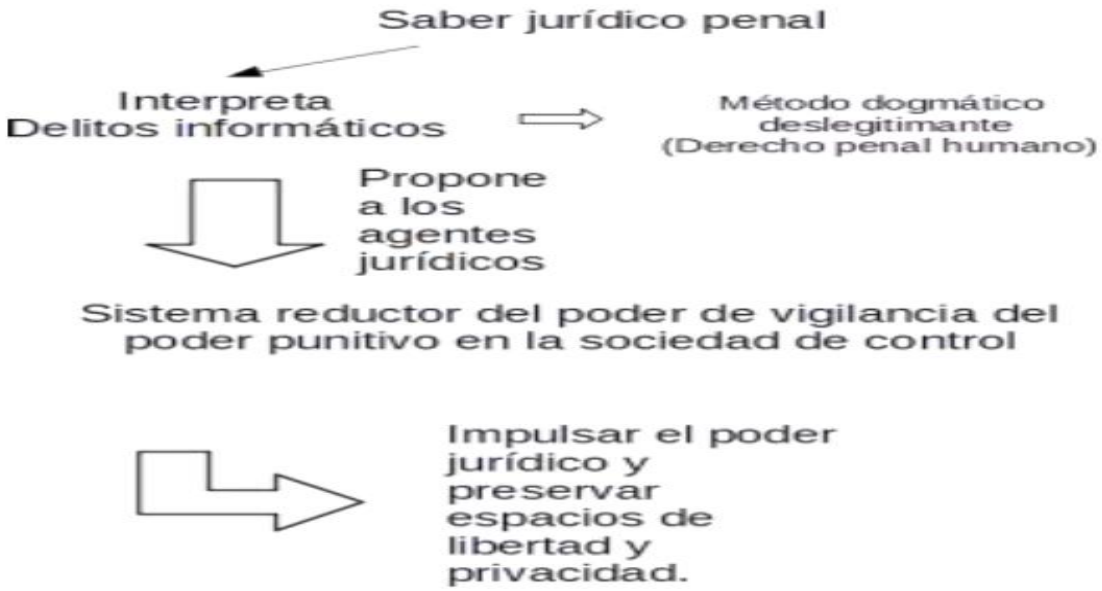
El estudio de Elías (2014) tuvo por objetivo realizar un diagnóstico sobre la problemática que genera los delitos informáticos y las normas con que se cuentan. El estudio de enfoque cuantitativo, obtuvo como resultado que el país posee una legislación insuficiente para contrarrestar los efectos negativos de este delito. El autor concluye que, pese a que el Perú no se sabe de cifras ciertas que evidencian el daño económico que supone este tipo de delitos, aunque sí se requiere indicar que recientemente este delito ha aumentado de modo significativo a nivel nacional, siendo Lima el lugar con el mayor porcentaje de casos denunciados. Ello se explica por la densidad poblacional que habita en esa ciudad, pero además porque muchas de ellas cuentan con algún dispositivo informático. Este estudio aportó en el análisis cualitativo y cuantitativo de nuestra propia investigación.

Epistemología de la problemática investigada. Delito de fraude informático El delito de fraude informático encuentra sus orígenes legales en el delito de acceso ilícito, promulgado en 1984, por el Congreso norteamericano, en ella se restringió el acceso a todo modo de difusión de datos que además de penalizar los daños económicos, protegía la seguridad pública y el secreto de los negocios, puesto que la preocupación por el valor de la data fue siempre relevante para el mundo.

Antes de precisar los alcances teóricos del delito de fraude informático es necesario precisar lo referido a las características del Derecho Penal Informático humano, estas son: a) Sancionatoria: el que sanciona es la norma penal (Zaffaroni), b) Personalismo: porque el destinatario de la ley es el infractor a quien se le aplica la pena, c) Valorativo: por los juicios de valor sobre las acciones humanas regulados en la norma, d) Finalista: ya que la norma penal busca resguardo de los bienes jurídicos con implicancia penal, el Derecho Penal informático, en cuanto saber penal, es además finalista, cuando genera la diminución del poder punitivo en un país (Balestra, citado por Espinoza, 2017).

Estas características se grafican de la siguiente manera.

Figura 1
Características del Derecho Penal Informático humano



Fuente: Extraído del libro Derecho Penal Informático: deslegitimación del poder punitivo en la sociedad de control, cuyo autor es Espinoza (2017, p. 28).

Dicho lo anterior, nos puede quedar claro que el delito informático es denominado de modo (a) formal, como acción u omisión limitada por la norma sobre delitos informáticos; (b) material, como acción que vulnera derechos vinculados a las TICs y (c) analítica, como acción típica, antijurídica y culpable que posee como modo de salvaguarda a las TICs (Espinoza, 2014).

Como todo delito informático, el fraude informático, se clasifican en dos categorías:

1) Como medio: son las acciones que usan las computadoras (PC) como modo en la realización del ilícito, como: a) Falsificación de data digital, b) modificación de los activos y pasivos en la contabilidad de los negocios, c) Planeación o simulación de ilícitos comunes, d) "Robo" de tiempo de PC, e) Lectura, sustracción o copiado de data secreta, f) cambios en la información en la entrada y salida. g) violación de un código para acceder a un sistema con medios ilegales,

h) cambios del destino de pocos montos de dinero hacia una cuenta bancaria apócrifa, i) Uso ilegal de programas cibernéticos, j) Inclusión de reglas que generan "interrupciones" en el manejo interno de los sistemas, a fin de conseguir ventajas ilícitas, k) modificación en el manejo de los programas, l) Obtención de dato residual impresa en papel o cinta magnética luego de la realización de labores, m) Acceso a áreas cibernéticas sin autorización, n) Interceptación en las líneas telefónicas.

2) Como fin: son las acciones orientadas en contra de la PC, programas como medio físico: a) Programas que bloquean total o parcialmente al sistema, b) Destrucción de programas por cualquier medio, c) Daño a la memoria, d) afectación física contra la PC o sus accesorios; e) Sabotaje político o terrorismo en que se vulnere o surja un uso de los centros de cómputo centrales, f) Secuestro de soportes magnéticos en los que se ubique data importante con fines de chantaje, pago de rescate, etc. (Téllez, 2008).

Otra clasificación de este tipo de delitos es el que propone Migliorisi (2014). Este autor señala dos grupos:

1) Ilícitos típicamente informáticos: son los que no fueran posibles sin la informática, infecciones informáticas a través de virus, programas dañinos orientados a la denegación de servicio e ilícitos vinculados con marcas y patentes y la identificación de los sujetos, y

2) Delitos realizados a través de internet: calumnias, extorsiones, estafas, hurto informático, violación de correspondencia, instigación a cometer delitos, ejercicio ilegal de profesiones, delitos contra la propiedad intelectual, *grooming, cyberbullyng, spoofing,* incitación a la violencia y distintos modos de delitos sexuales (pedofilia, pornografía infantil y corrupción de niños).

En el Perú, el delito de fraude informático se incluyó en el art. 8 de la Ley de delitos informáticos y luego modificado por la Ley 30171, que señala: el que deliberada e ilegítimamente procura para sí o para otro un beneficio ilícito para dañar a un tercero a través del diseño, introducción, alteración, borrado, supresión,

clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema digital, será reprimido con pena privativa de libertad no menor de tres ni mayor de ocho años y con 60 a 120 días-multa. La pena será privativa de libertad no menor de 5 ni mayor de 10 años y de 80 a 140 días-multa cuando se vulnere el patrimonio público orientado a fines humanitarios.

Figura 2
Comparación del delito de fraude informático en la Ley N° 30096, Ley 30171 y el Convenio de Budapest

Ley No. 30096	Ley No. 30171	Convenio de Budapest
Art. 8 LDI.- El que, a través de las tecnologías de la información o de la comunicación, procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.	Art. 8 LDI.- El que deliberada e ilegítimamente procura para sí o para otro un provecho ilícito en perjuicio de tercero mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático, será reprimido con una pena privativa de libertad no menor de tres ni mayor de ocho años y con sesenta a ciento veinte días multa. La pena será privativa de libertad no menor de cinco ni mayor de diez años y de ochenta a ciento cuarenta días multa cuando se afecte el patrimonio del Estado destinado a fines asistenciales o a programas de apoyo social.	Art. 8.- Las Partes adoptarán las medidas legislativas o de otro tipo que resulten necesarias para tipificar como delito en su derecho interno los actos deliberados e ilegítimos que causen perjuicio patrimonial a otra persona mediante: a. la introducción, alteración, borrado o supresión de datos informáticos; b. cualquier interferencia en el funcionamiento de un sistema informático, con la intención, dolosa o delictiva, de obtener de forma ilegítima un beneficio económico para uno mismo o para otra persona.

Fuente: Extraído del libro Luces y sombras en la lucha contra la delincuencia informática en el Perú, cuyo autor es Elías (2014, p. 81).

El delito de fraude informático posee las siguientes características:

1) Acciones criminales de alto vuelo, porque cierto número de personas con determinados saberes especializados pueden realizarlas,

2) Conductas ocupacionales ya que por lo general se hace cuando la persona está laborando;

3) Conductas de oportunidad, ya que se beneficia de una situación inventada o intensificada en la operatividad del sistema tecnológico y económico;

4) Generan una alta pérdida económica;

5) Se hacen con facilidad de tiempo y espacio ya que pueden realizarse en corto tiempo y sin que sea necesario la presencia física,

6) Difícil comprobación, ya que los causantes realizan de modo anónimo haciendo uso de servidores *proxys*, email anónimo, direcciones IP dinámicas, conectado por *wifi*, de esta manera, la cifra de autores de este ilícitos es incierta, lo único que se sabe es de la presencia de *bitcoins;*

7) Sofisticados y casi recurrentes en el campo profesional,

8) Son de difícil comprobación, por ser especializado;

9) Por lo general son dolosos, aunque también los hay culposos;

10) Tienden a extenderse, por lo que se necesita una normativa en el plano mundial;

11) De mera actividad y con presencia del hecho, pueden repetirse de modo constante en el tiempo, ya que se realizan de modo instantáneo, se planifican con la actividad u omisión, no se necesita el perjuicio, sus consecuencias son constantes;

12) Pluriofensivos y masivos: podrían dañar distintos bienes jurídicos y a distintos sujetos pasivos;

13) Transfronterizos: usan la internet, por lo que puede tener consecuencias en distintos lugares del mundo (Téllez, 2008; Acosta, 2003).

Respecto a la tipología de los fraudes informáticos estos son los siguientes:

a) Entrada de datos falsos o engañosos: es la manera más simple, que supone modificar los datos antes o durante su ingreso en la PC, Parker (1989) lo ejemplifica así: cualquier persona que posea acceso a los procedimientos de creación, grabación, transporte, codificación, examen, comprobación, conversión y transformación de data que ingresan a una PC puede modificar dicha data;

b) manipulación de software: es la colocación encubierta o la modificación de las reglas de la PC o los datos en un sistema para que el equipo desarrolle acciones ilícitas, por lo general aún posibilitan que el sistema haga la mayoría o todos los fines previstos (Parker, 1989);

c) Técnica del Salami: es una modalidad automatizada de abuso ejecutando un sistema ilegal con el objetivo de obtener datos activos sin reducir el total de estos (Parker, 1989);

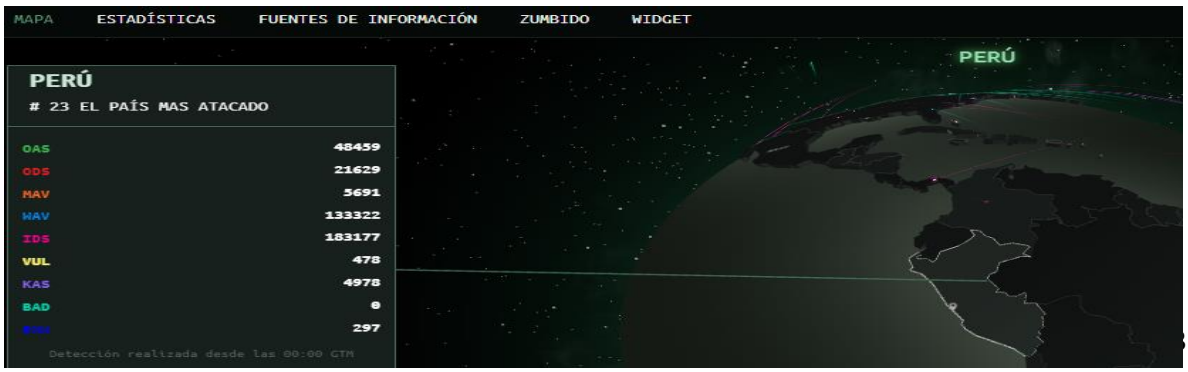
d) Falsificaciones informáticas: se tiene como fin, cuando se cambia información de los documentos guardados de manera virtual; y, como instrumento, cuando las PC pueden usarse para falsificar documentos de negocios (Magro Servet, 2010);

e) Manipulación de data de la salida: se hace señalando un objetivo al funcionamiento del sistema. Por ejemplo: el fraude de que se hace objeto a los cajeros automáticos a través de la falsificación de reglas para la PC en la fase de obtención de data (Hall, 2010);

f) El *Pishing* y el hurto o robo de identidad: el primero implica obtener por fraude, datos secretos, haciéndose pasar por una persona o empresa de confianza a través de una comunicación virtual de apariencia oficial *(email, SMS*, página web clonada), (ITU, 2009), y el segundo ocurre cuando alguien obtiene data perteneciente al afectado y se hace pasar por él (Gercke, 2013).

De acuerdo a cybermap.kaspersky.com el Perú es el 23 país más atacado del mundo con virus informáticos o software que buscan información de las personas, tal como se aprecia a continuación.

Figura 3
Ciberataques en Perú, agosto, 2021



Fuente: https://cybermap.kaspersky.com/es

Cybermap.kaspersky.com también precisa cuáles son las amenazas cibernéticas que recibe el Perú en tiempo real, como se detalla a continuación:

Figura 4
Amenazas cibernéticas en Perú, agosto, 2021

Fuente: https://cybermap.kaspersky.com/es

Análisis de la legislación. A nivel internacional se cuenta con el Convenio de Budapest o Convenio sobre la ciberdelincuencia, aprobado el 2001. En esa línea, cabe señalar que el Código Penal cuenta con un Capítulo de Delitos Informáticos,

el mismo que se ha ido conformando a partir de la Ley N° 27309 que reguló el delito informático (art. 207-A del Código Penal - CP), el delito de alteración, daño y destrucción de base de datos, sistema, red o programa cibernéticos (art. 207-B del CP) y el delito informático agravado (art. 207-C del CP). También se cuenta con la Ley N° 30171 del 10 de marzo de 2014.

Haciendo un comparativo, sobre los delitos contra datos y sistemas informáticos, entre la Ley 30096, la Ley 30171 y el Convenio de Budapest, se puede precisar lo siguiente.

Figura 5
Comparación entre la Ley 30096, Ley 30171 y el Convenio de Budapest

Ley No. 30096	Ley No. 30171	Convenio de Budapest
Art. 2 LDI.- El que accede sin autorización a todo o en parte a un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.	**Art. 2 LDI.-** El que **deliberada e ilegítimamente** accede a todo o en parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecida para impedirlo, será reprimido con pena privativa de libertad no menor de uno ni mayor de cuatro años y con treinta a noventa días-multa. Será reprimido con la misma pena el que accede a un sistema informático excediendo lo autorizado.	**Art. 2.-** Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno el acceso deliberado e ilegítimo a todo o parte de un sistema informático. Las Partes podrán exigir que el delito se cometa infringiendo medidas de seguridad, con la intención de obtener datos informáticos u otra intención delictiva, o en relación con un sistema informático conectado a otro sistema informático.
Art. 3 LDI.- Atentado a la integridad de los datos informáticos. El que, a través de las tecnologías de la información o de la comunicación, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.	**Art. 3 LDI.-** El que **deliberada e ilegítimamente daña,** introduce, borra, deteriora, altera, suprime o hace inaccesible datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.	**Art. 4.-** 1. Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno todo acto deliberado e ilegítimo que dañe, borre, deteriore, altere o suprima datos informáticos. 2. Las Partes podrán reservarse el derecho a exigir que los actos definidos en el párrafo 1 comporten daños graves.
Art. 4 LDI.- El que, a través de la tecnología de la información o de la comunicación, inutiliza total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.	**Art. 4 LDI.-** El que **deliberada e ilegítimamente** inutiliza, total o parcialmente, un sistema informático, impide el acceso a este, entorpece o imposibilita su funcionamiento o la prestación de sus servicios, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.	**Art. 5.-** Cada Parte adoptará las medidas legislativas y de otro tipo que resulten necesarias para tipificar como delito en su derecho interno la obstaculización grave, deliberada e ilegítima del funcionamiento de un sistema informático mediante la introducción, transmisión, daño, borrado, deterioro, alteración o supresión de daños informáticos.

Fuente: Extraído del libro Luces y sombras en la lucha contra la delincuencia informática en el Perú, cuyo autor es Elías (2014, p. 92).

Naturaleza del delito de fraude informático, esta es una modalidad que se origina con el delito de acceso ilícito. El contenido del injusto del hecho típico, surge como un tipo de acceso ilícito no tan grave, fue aumentando cuando tiene que ver con daño económico.

Respecto a los sujetos: 1) El sujeto activo, es una persona natural, 2) El sujeto pasivo, es una persona natural o jurídica, también puede ser el Estado. El artículo 11 de la Ley de delitos informáticos, le da mayor pena al autor cuando es miembro de una organización criminal, abusa de una posición de acceso a la data reservada o al conocimiento de esta data por el cargo que ostenta.

Sobre el tipo objetivo sistemático. La exteriorización de la acción. Según el artículo 1 del Convenio de Budapest, se entiende por Sistema Informático todo dispositivo aislado o conjunto que estén interconectados entre sí, siempre que uno o varios de ellos posibilite el abordaje automatizado de datos en aplicación de un sistema.

Los datos informáticos es cualquier representación de acciones, información de manera que permita el abordaje del tratamiento informático, incluso un sistema hecho para que un sistema informático aplique una acción. Por datos sobre el tráfico entiéndase a cualesquier dato informático relativo a una comunicación a través de un sistema informático, ocasionados por un sistema informático, que indique el origen, destino, ruta, hora, fecha, tamaño y duración de la comunicación, el tipo de servicio; el tipo prohíbe que de modo intencionado e indebido o contra la ley, se procure para sí o para otro un beneficio ilegal perjudicando a un tercero a través del diseño, introducción, alteración, borrado, supresión, clonación de data informática o cualquier interferencia o manipulación en el procesamiento de un programa informático, con el agravante de que si se afecta el patrimonio estatal orientado a fines humanitarios.

El hecho de interceptar datos, es de resultado (Villavicencio, 2015), por tanto, se consuma cuando se genera la afectación patrimonial a un tercero con la utilización ilícita para sí o para otro, con la realización de cada uno de los tipos penales (BBC Mundo, 2017).

De la fórmula del tipo penal se entiende que el bien jurídico es el patrimonio, ya que después de las operaciones fraudulentas, se ocasiona un daño económico, puesto que se obtiene un movimiento económico a su favor afectando los datos y sistemas informáticos que los contienen.

Mientras que el dolo, es la voluntad que aplica el tipo orientada por el saber de los aspectos del tipo objetivo sistemático (Zaffaroni, 2009), por ello el agente debe conocer y querer cada uno de los aspectos del tipo objetivo sistemático a fin de que se le aplique una imputación directa, respetando el principio de legalidad, ello supone que el sujeto posea habilidades informáticas, de ya tenerlos, agravaría la vulnerabilidad de los agentes frente al poder punitivo, de modo que el solo utilizar las TIC, los haría delincuentes en potencia.

El artículo 11 de la Ley de Delitos Informáticos, le da mayor sanción al autor cuando acciona con el propósito de conseguir una ventaja económica, esto supone que el objeto del delito, debe ser susceptible de cuantificación económica a fin de justificar el *animus lucrandi*.

Sobre la concurrencia y participación, esta es posible que surja un concurso aparente con diferentes delitos, empezando por los de la misma ley de delitos informáticos como el acceso ilegal, al momento de acceder al sistema para realizar operaciones, el atentado contra información y sistemas informáticos porque en dichos ilícitos, se actúa de manera similar al fraude informático, aunque hay la voluntad de obtener beneficio ilícito para sí o para otro, también entraría en concurso real los delitos contra el patrimonio (hurto). Finalmente, el tipo penal, acepta la coautoría y la participación de cómplices e instigadores (Espinoza, 2017).

E-comerce. Cuando se habla de comercio electrónico es indispensable considerar qué es lo que el concepto supone y sus diferentes connotaciones. El término *E-comerce* surge para identificar a todos aquellos negocios en las que participan

medios electrónicos. Este concepto supone más allá de la venta por medios digitales. El comercio electrónico como cualquier otro negocio se sustenta en la transmisión de datos sobre redes de comunicación. Este término no sólo se refiere a la compra y venta electrónica de bienes y servicios, sino también al uso de la red para publicidad, búsqueda de datos sobre productos o atención al consumidor antes y después del negocio (Asturias Corporación Universitaria, 2018 y Sánchez, 2005).

Es necesario considerar el directo vínculo que tiene con la tecnología, puesto que es ésta quien posibilita funcionar los programas de comercio virtual. En este proceso nos encontramos con un alto número de medios tecnológicos.

Como todo negocio, el *e-comerce*, tiene ventajas y desventajas. Veamos.

1) Sobre los beneficios del *E-comerce* desde el punto de vista del negocio este posibilita la ampliación del mercado: Lanzarse a una plataforma *online* puede contribuir a los negocios a ampliar su mercado, siendo un buen modo para la internacionalización del negocio. Por este alcance mundial de internet es posible que cualquier empresa independiente de su dimensión y ubicación se abra al planeta a través del *E-comerce*.

2) Eliminación de las limitaciones de horarios: En gran parte de los lugares, las tiendas físicas poseen límites de horarios comerciales con horas y días donde existen límites. Esto es algo que no sucede con el comercio online, permitiendo una tienda abierta 24 horas, durante toda la semana, lo que permite que los horarios no sean una limitación para la empresa.

3) Mejoras en los procesos: ya que posibilita a las empresas mejorar en cuanto a la optimización de solicitudes, así como en la verificación de stocks y pedidos. Para ello, el medio tecnológico es clave, de modo que, si un negocio tiene implementado un buen sistema de control, el *E-comerce* va a posibilitarle mejorar el rendimiento del negocio.

4) Ahorros en costes: las ventas online también implican un ahorro en costes al no requerir de mantenimiento de una tienda física con los gastos que esto

supone; así como gastos de personal. Esto no quiere decir que un negocio virtual no necesite de personal ni que no genere gastos, sino que éstos están muy por debajo de los costos que genera una tienda física.

5) medio de venta alternativo: Este negocio puede ser un buen modo de venta extra que suma a un negocio físico. De esta manera es posible, buscar unos ingresos extra para el negocio físico y aprovechar los recursos en la coyuntura con menos actividad en la tienda física, para dirigirlos al negocio virtual, mejorando así la capacidad de la empresa.

Respecto a las desventajas, estas son:

1) Dependencia de la tecnología: Cualquier empresa que se sostenga en el *E-comerce*, estará dependiente de que la tecnología funcione de modo óptimo, de manera que cualquier problema afectará a la empresa y por tanto dificultará a la empresa, pues gracias al intercambio de datos se produzca, impactando de manera negativa.

2) Distribución: Cuando se refiere a productos físicos, una vez realizado las solicitudes, se necesita distribuirlo. Para ello, los negocios pueden contar con su propia distribuidora. En este caso, el producto tendrá un plazo de entrega que, cuanto mayor sea, hará menos satisfactoria, además del gasto que esto genera.

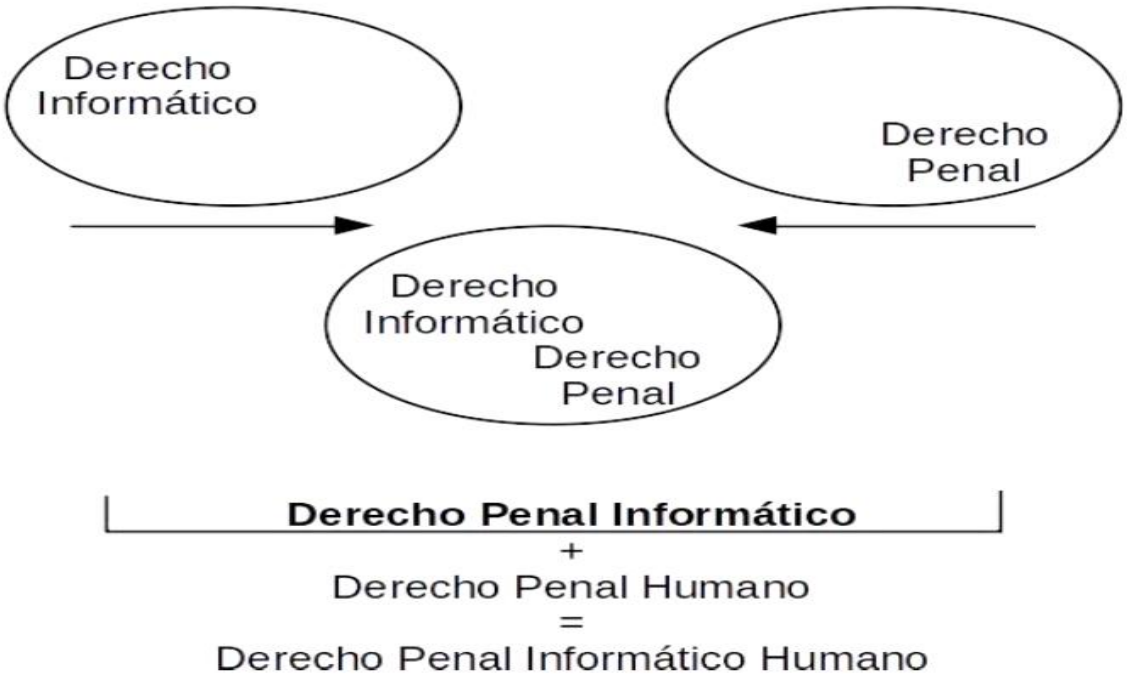
3) Seguridad: El *E-comerce*, al sustentarse en internet, depende de las limitaciones de la red en cuanto a la seguridad y, a pesar de que los esfuerzos en este sentido aumentan y cada vez es más segura, siempre existe un riesgo que pone en peligro el buen funcionamiento de la plataforma, así como la seguridad de la data.

4) Frenos en los consumidores: Si bien cada vez es más grande el consumidor online, aún hay amplios sectores poblacionales que no les interesa comprar a través de medios virtuales (Asturias Corporación Universitaria, 2018).

Rol del Ministerio Público

El Ministerio Público tiene claro la interdisciplinariedad que existe entre el Derecho Informático y el Derecho Penal, la suma de ambas junto con el Derecho Penal Humano, conllevan a la configuración del Derecho Penal Informático Humano, esto se grafica de la siguiente manera:

Figura 6
Interdisciplinariedad entre el Derecho Informático y el Derecho Penal



Fuente: Extraído del libro Derecho Penal Informático: deslegitimación del poder punitivo en la sociedad de control, cuyo autor es Espinoza (2017, p. 90).

Esto quiere decir que, ante los delitos informáticos, el rol del Ministerio Público se hace más complejo y exigente ya que se requiere de fiscales más capacitados, empoderados en manejo de los medios digitales, informáticos y cibernéticos. De no ser así, el ciberdelito seguirá en aumento, la impunidad será campante y los bienes jurídicos de las personas estarán en riesgo. En ese sentido, creemos que un abordaje interdisciplinario y estratégico contribuirá a fortalecer las acciones e investigaciones contra este delito.

Lo anterior implica que el Estado debe asignar los recursos logísticos, humanos y económicos para que el Ministerio público cuente con equipos de tecnología de punta, servicios de conectividad de alto alcance, computadoras y medios cibernéticos suficientes para todos, personal debidamente capacitado y especializados a fin de manejar software y programas cibernéticos, además de una infraestructura adecuada para todo ello. Esto además permitirá realizar un trabajo coordinado con la Policía Nacional, en particular con la División de Investigación de Delitos de Alta Tecnología.

División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú (**DIVINDAT)**

Esta División policial fue creada mediante Resolución Directoral N° 1695-2005-DIRGFN/EMG del 2005, a fin de que esta Unidad investigue los ilícitos informáticos y esos casos en los que se utilicen medios digitales para la realización de otros ilícitos (difusión de pornografía infantil, fraudes electrónicos, hurtos de fondos, etc.), en particular los que señalaba la Ley 27309.

Se trata de una División altamente especializada y que realiza labores y operativos planificados y estratégicos, en coordinación con el Ministerio Público. Cabe señalar que la implementación de esta División ha conllevado a que los efectivos policiales se capaciten y desarrollen competencias digitales que les permita usar mejore los recursos y medios cibernéticos y digitales, además esto ha supuesto una inversión importante en recursos logísticos, infraestructura y económicos. De tal modo, que la Policía cuenta con una instancia especializada y que realiza una labor sistemática para enfrentar los efectos del ciberdelito a nivel nacional.

Según el art. 2 de la citada Resolución, la DIVINDAT como instancia especializada de la Policía realiza una labor articulada al interior y el exterior de la institución, en particular con el Ministerio Público y el Poder Judicial. Esta División está integrada por tres departamentos y una de ellas, a su vez, por cuatro secciones que se detallan a continuación.

Figura 7

Organigrama de la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú

Fuente: Extraído del libro Luces y sombras en la lucha contra la delincuencia informática en el Perú, cuyo autor es Elías (2014, p. 102).

Marco conceptual

Delito: es una conducta típica, antijurídica y culpable (Zaffaroni, 2009).

Delito informático: es la acción u omisión prohibida por la norma; material, acción final que vulnera bienes jurídicos analizados por el Derecho informático, como acción típica, antijurídica y culpable que tiene como medio a las tecnologías de la información y la comunicación. Este delito tiene funciones, características y una clasificación, diferente a los otros ilícitos.

Criminalidad informática: se trata de un asunto jurídico que tiene por objeto afectar los programas de modo integral, como los ataques de tipo r*ansomware*, secuestrando datos a cambio de b*itcoins*, para liberar los sistemas hospitalarios, de telefonía, PC, laboratorios, planta nuclear, entre otros (DW, 2017, Infobae, 2017, BBC Mundo, 2017).

Derecho Penal Informático: es el saber jurídico-penal, que, a través de la interpretación de las normas sobre delitos informáticos, propone un sistema orientador de decisiones que asume y disminuye el poder sancionador, para normalizar la sociedad de control y fortalecer el Estado Constitucional de Derecho. El Derecho Penal Informático es de tipo público, normativo, continuo, represivo y fragmentario del poder punitivo del Estado (Espinoza, 2017).

Ley N° 30096: aprobada el 22 de octubre de 2013 conocida como Ley de Delitos Informáticos (LDI). También se le denomina como Ley de represión de la cibercriminalidad.

Sistemas informáticos: son todo dispositivo aislado o conjunto de dispositivos interconectados entre sí, cuya función, o la de alguno de sus elementos, sea para el tratamiento automatizado de información en ejecución de un programa (Convenio de Budapest o Convenio sobre la Ciberdelincuencia).

Datos informáticos: es toda representación de hechos, información o conceptos manifestados por cualquier modo que se preste a tratamiento informático, incluidos los sistemas generados para que un programa virtual aplique una acción (Convenio de Budapest o Convenio sobre la Ciberdelincuencia).

III. METODOLOGÍA

3.1. Tipo y diseño de investigación

El presente estudio estuvo estructurado de acuerdo al tipo de estudio básico ya que parte de un conocimiento previo, para luego aplicar lo que señalan Hernández, Fernández y Baptista (2014) este estudio aprecia lo que ya está aconteciendo y, por tanto, debe asumirse que no fue provocado por el agente por lo que las categorías de estudio no se pueden manipular porque ya ocurrieron.

Para Hernández el diseño de la investigación es el plan que se aplica para obtener la data que se necesita en un estudio (2007). Para efectos de esta investigación fue de diseño de Teoría Fundamentada, que fue el más apropiado de un enfoque cualitativo y de tipo básico. Con estos aspectos metodológicos se aseguró una investigación de relevancia científica.

3.2. Categorías. Sub categorías. Matriz de Categorización

Las categorías a estudiar fueron las siguientes:

Tabla 1
Categorización

Categorías	Definición conceptual	Sub categoría
Categoría 1: El delito de fraude informático	Se define como una manera (a) formal, como acción u omisión sancionada por la norma sobre delitos informáticos; (b) material, como acción final que vulnera bienes jurídicos relacionados a las TICs, y (c) analítica, como acción típica, antijurídica y culpable que tiene como medio de resguardo a las TICs (Espinoza, 2014).	Subcategoría 1: Ciberdelincuencia
		Subcategoría 2: Ley N° 30096 y su Reglamento
Categoría 2: *E-comerce*	Es la distribución, producción, comercialización, venta o entrega de bienes y servicios de manera virtual (Organización Mundial del Comercio, 1998).	Subcategoría 1: Labor del Ministerio Público
		Subcategoría 2: Labor de la Policía Nacional

3.3. Escenario de estudio

Fueron tres los escenarios de estudio de la presente investigación, a saber:

1) El Ministerio Público de Lima centro,

2) La Oficina Técnica del Ministerio Público,

3) La División de Investigaciones de Delitos de Alta Tecnología de la PNP.

Estas tres instancias tienen competencias sobre la problemática estudiada, y se acudió a ellas para recabar información y datos que posteriormente fueron analizadas.

3.4. Participantes

La población a estudiar estuvo ubicada en el territorio nacional, en la ciudad de Lima, en consideración de que la investigación busca analizar la problemática expuesta de modo directo y actual.

A partir de ello se elaboró una muestra poblacional, con los siguientes participantes.

a) **Los fiscales del Ministerio Público de Lima centro**. Resultó necesario entrevistar a dichos funcionarios a fin de recabar de ellos, la información que tienen respecto al delito de fraude informático cometido a través del *E-comerce* y la ciberdelincuencia.

b) **Los funcionarios de la Oficina Técnica del Ministerio Público** en donde ellos con su experiencia dieron alcances para contar con un estudio preciso de lo que estuvo ocurriendo respecto al delito de fraude informático cometido a través del *E-comerce* y la ciberdelincuencia.

c) **Los efectivos policiales**: en particular de la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional, a fin de obtener de ellos la casuística necesaria que permitió comprender y explicar el fenómeno.

d) **Los expertos:** especialistas en el delito de fraude informático cometido a través del *E-comerce* y la ciberdelincuencia.

La siguiente tabla precisa el perfil académico de los participantes:

Tabla 2
Informantes claves

Perfil Académico		
Puesto que desempeña	**Años de Experiencia en la Materia**	**Nivel Educativo**
Se tuvo en cuenta el puesto que desempeña en el Ministerio Público, en la Policía Nacional, catedrático, abogado litigante.	Para el desarrollo de la entrevista, se consideró el tiempo de experiencia en el Derecho Penal, procesal y ciberdelitos.	Para el desarrollo de la entrevista, se consideró el nivel educativo: debiendo ser titulado, Magister o Doctor en Derecho.

3.5. Técnicas e instrumentos de recolección de datos

1) **Análisis de fuente documental**: Se hizo un amplio análisis documental de la norma, expedientes, casuística actual, las cuales se expresan en las conclusiones. Se recopiló data de distintos estudios, y en el caso de la presente investigación se indagó la doctrina en materia del Derecho Penal. El análisis de fuente documental es el tipo de técnica que se realiza basándose en fuentes escritas, principalmente (Behar, 2008).

2) **Entrevista**: es una técnica que se aplicó a expertos en el tema y con preguntas abiertas. Se realizó entrevistas a los funcionarios del Ministerio Público, Policía Nacional, expertos y abogados especializados en Derecho Penal e informático.

3.6. Procedimientos

El procedimiento metodológico que conlleva realizar el presente estudio fue el siguiente:

1) Elección de la problemática de estudio.

2) Búsqueda de datos en repositorios y base de información.

3) Formulación de objetivo e hipótesis.

4) Elección del tipo, enfoque, diseño de estudio.

5) Recopilación de la información a través de un trabajo de campo: entrevista a expertos.

6) Procesamiento de la información en Resultados y Discusión.

7) Elaboración de conclusiones y recomendaciones.

8) Sustentación del estudio ante jurado calificador. Levantamiento de observaciones.

3.7. Rigor científico

Para asegurar el rigor científico se plantearon el uso de diversos componentes que a continuación explicamos:

Uso del cuestionario: De modo complementario se usó el cuestionario para la obtención de datos precisos, para ello este medio fue dirigido a partir de preguntas cerradas y sistemáticamente ordenadas en relación a los objetivos.

Validez y confiabilidad de los instrumentos: se realizó por medio del juicio de expertos, los cuales analizaron cada uno de los Ítems formulados, como parte del cuestionario diseñado.

Confiabilidad: se respaldó en su originalidad, elaboración y la respectiva validación de la ficha de los instrumentos evaluados por el juicio de expertos, sobre todo en metodología y temático.

Enfoque Cualitativo: la presente Investigación es de tipo cualitativo porque hemos desarrollado de modo teórico y práctico. El uso de métodos cualitativos para desarrollar investigaciones nos permitió abordar hechos concretos del fenómeno y como éstos se desarrollaron; es decir, dentro de su contexto real. Estos métodos se enfocan a describir la esencia del contexto dado entre los participantes (Hernández, 2007).

3.8. Métodos de análisis de datos

La presente investigación se basó en un método analítico puesto que lo que se buscó fue describir el fenómeno jurídico del ciberdelito, sobre todo, del que se realiza con el *E-comerce*. Sin dejar de lado el método de análisis de datos que se llevó a través del uso de los medios de obtención de información; paramétrico, elaborando y aplicando las respectivas herramientas de obtención de información con el fin de conseguir la información necesaria acerca del fenómeno, asimismo se tomó en cuenta distintas posturas y perspectivas acerca del problema asumido, en atención a los fines fijados en este estudio, y finalmente se contrastó las hipótesis, habiendo analizado y discutido previamente la data contrastada.

3.9. Aspectos éticos

Para este estudio se tuvo en cuenta la veracidad de resultados; se respetó la propiedad intelectual; la responsabilidad social, política, jurídica y ética; se respetó la privacidad de los participantes; se protegió su identidad cuando así lo solicitaron. Asimismo, la presente investigación se desarrolló bajo los aspectos metodológicos estipulados por la Universidad y la Ley Universitaria, considerando la imparcialidad sobre el tema; por consiguiente, el acatamiento al método científico planteado por lo que la presente investigación se sustenta bajo los aspectos éticos propios de una investigación científica, considerando además las indicaciones brindadas por el asesor metodológico y el esquema propuesto por la Universidad. Del mismo modo, el uso adecuado de las normas de citado de la Asociación de Psicología Americana. Finalmente, declaramos que hubo ningún conflicto de interés con el tema abordado, ni con los participantes ni el lugar o escenario de estudio, con lo que se aseguró la imparcialidad y objetividad de los resultados.

IV. RESULTADOS Y DISCUSIÓN

4.1. Descripción de resultados de la técnica: Entrevista a expertos

A continuación, se presentan los datos obtenidos de la técnica de entrevista, tomando en consideración los objetivos propuestos en el estudio. Cabe señalar que los entrevistados fueron previamente informados de los alcances del estudio y dieron consentimiento para que la información brindada sea publicada en el presente estudio.

Tabla 3
Ficha técnica de entrevistados

N°	Entrevistado	Descripción
1	Luis Álvaro Cárdenas Moreno	Fiscal Provincial de la Sexta Fiscalía Provincial Penal Corporativa de Huancayo. Ministerio Público
2	Luis Humberto Mejia Izaguirre	Fiscal Adjunto Provincial Corporativo Especializado en Delito de Trata de Personas
3	Luis Gabriel Soca Rodríguez	Defensor Público del Ministerio de Justicia. Abogado. Lima Este
4	Kathia Montalván Castañeda	Fiscal Adjunto Provincial de la Quinta Fiscalía Penal Corporativa de Huancayo
5	José Luis Baquerizo Haro	ST1 PNP – DIVINDAT – DIRINCRI PNP
6	José Bustamante	S3 PNP – DIVINDAT – DIRINCRI PNP
7	Víctor Espinoza Prado	S1 PNP – DIVINDAT – DIRINCRI PNP
8	Julio Ronald Larico Rodríguez	S2 PNP – DIVINDAT – DIRINCRI PNP
9	Andrea Rodríguez Flores	S1 PNP – DIVINDAT – DIRINCRI PNP
10	José Miguel Millones Velásquez	S1 PNP
Entrevistas realizadas durante el mes de marzo de 2022, en la ciudad de Lima, de manera virtual y en algunos casos de manera presencial.		

Resultados del **objetivo general**: Determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-comerce* en la lucha contra la ciberdelincuencia en el periodo 2021, los resultados de la técnica de entrevista relacionados al objetivo general se plantearon del modo

siguiente. Respecto a la pregunta: ¿En qué consiste el fraude informático cometido a través del *E-comerce*?

Cárdenas Moreno señala que, en palabras sencillas, podría señalar que el fraude informático cometido a través del E-comerce no es nada más ni nada menos que la estafa cometida en el campo del E-comerce. Como es sabido el desarrollo de la tecnología como el internet así como las nuevas tecnologías de la información y comunicación (TICs) han hecho que nuestras vidas se conviertan en una vida más virtualizada, es así que el mundo del comercio no ha sido ajena a ello razón de la existencia de "E-comerce" comercio electrónico que ha permitido que muchas empresas pequeñas y grandes hayan podido realizar sus actividades comerciales a través del mundo electrónico tanto más en tiempos de pandemia en donde el distanciamiento social era imprescindible para la subsistencia de la vida humana; sin embargo, esta nueva vida comercial ha traído consigo riesgos y ataques en sus sistemas operativos no solo a las empresas que la utilizan sino también a los propios consumidores a través de este tipo de estafas cibernéticas, en donde una vez obtenidas sus datos informáticos registradas en dicha plataforma virtual, proceden a desviar tus fondos con o sin el consentimiento del titular, apropiándose así de manera ilegítima de su patrimonio.

Mejia Izaguirre sostiene que consiste en la alteración, supresión, distorsión o sustitución de información digital con la finalidad de obtener un beneficio ilícito en perjuicio de terceros en la realización de actividades o transacciones comerciales a través de internet, aplicaciones de celular y canales informáticos (comercio electrónico) entre los cuales tenemos los fraudes de clonación de tarjetas, transferencias electrónicas fraudulentas, *pishing,* robo de identidad, etc.

Soca Rodríguez manifiesta que consiste en la supresión, distorsión, alteración o sustitución de datos informáticos con la finalidad de obtener un provecho o ventaja ilícita en agravio de terceros, siendo el campo de acción de este flagelo en la transacción de actividades o transacciones comerciales a través de internet, aplicaciones de programas de teléfono celulares en el comercio

electrónico, por ejemplo, clonación de tarjetas de crédito, transferencias, compras fraudulentas y robo de identidad, *pishing,* entre otros.

Montalván Castañeda indica que son las clonaciones de tarjetas, trasferencias electrónicas fraudulentas, compras de internet a través de data de tarjeta de crédito o débito. Baquerizo Haro señala que consiste en el fraude informático que se efectúa al realizar compras y ventas de productos o servicios a través de internet o redes sociales. En su mayoría se observa que esta modalidad ocurre en la red social de Facebook o Mercado Libre. Bustamante indica que consiste en realizar compras por intermedio de una plataforma con la finalidad de obtener un producto sin la intervención de pagos o su valor, y así evitar el pago de la misma.

Espinoza Prado informa que ocurre cuando se compra con tarjeta de crédito o débito clonadas en la página web de una tienda virtual. Al ingresar a la página web de la tienda virtual y modificar la base de datos para realizar compras fraudulentas. Larico Rodríguez manifiesta que consiste en la creación de plataformas virtuales de comercio electrónico los cuales son mostrados a potenciales víctimas mediante publicidad engañosa, posicionamiento de búsqueda en Google y tienen como finalidad obtener información confidencial de tarjetas bancarias, contraseñas, claves Token, entre otros, los cuales son utilizados para cometer delito informático.

Millones Velásquez indica que son acciones cometidas a través del comercio electrónico caracterizado por la venta muy concurrida de las personas en las plataformas de internet. Rodríguez Flores menciona que es una operación que se realiza a través de internet mediante el cual se fijan operaciones (compras) que posiblemente nunca se concreten. Esta modalidad podría mal llamarse fraude informático, pero se trata de una estafa, vale decir que si el autor fabrica una página con el fin de realizar e-comerce, este se configura como delito informático.

Respecto a la pregunta: ¿Cuál fue el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del E-comerce en la lucha contra la ciberdelincuencia? Señalaron:

Cárdenas Moreno señala que el papel, que juega el MP, así como en los otros delitos comunes es la lucha contra esta y la prevención de la misma y esta persecución penal frente a esta modalidad delictiva está regulada a través de la Ley 30096 y su posterior modificación Ley N° 30171, que tiene por finalidad combatir los delitos informáticos, en el caso puntual que estamos tocando el fraude informático está regulado en el artículo 8° de esta ley, que señala: "El que deliberadamente procura para así o para otro un provecho ilícito mediante el diseño, introducción (...) de datos informáticos o cualquier interferencia o manipulación en el funcionamiento informático, será (...) la modalidad más frecuente en este medio "comercio electrónico" es el que se manifiesta a través del conocido "phishing" en donde el ciberdelincuente lo que hace es obtener los datos informáticos registrados en dicha plataforma para luego de ello haciendo un uso ilegítimo del mismo apropiarse de su patrimonio económico de sus víctimas.

Mejia Izaguirre sostiene que por mandato constitucional al Ministerio público le corresponde dirigir la investigación del delito con el apoyo de la Policía. Con respecto al fraude informático en el comercio electrónico, el Ministerio Público ha creado las fiscalías especializadas en ciberdelincuencia con la finalidad de combatir con más eficazmente este tipo de ilícitos.

Soca Rodríguez manifiesta que el Ministerio Público es el persecutor del delito, es decir, inicia y formaliza la investigación penal por mandato constitucional y mediante su Ley Orgánica. Para estos delitos informáticos, tiene como apoyo a las Unidades Especializadas en ciberdelitos de la Policía con la finalidad de luchar contra la delincuencia que está avanzando a pasos agigantados. Montalván Castañeda indica que se debe basar en la implementación de la logística y capacitación del personal fiscal en esta clase de delitos.

Baquerizo Haro señala que debe trabajar de forma conjunta con la División de delitos informáticos de la Policía Nacional para combatir el delito informático. Bustamante indica que evaluar la conducta en base a la denuncia recibida por medio de la PNP o el Ministerio Público. Espinoza Prado informa que el rol del Ministerio es la defensa de la legalidad y orienta para la obtención de las pruebas,

en el ejercicio oportuno de la acción penal. Larico Rodríguez manifiesta que se creó la Fiscalía especializada contra la ciberdelincuencia para investigar de modo específico y en conjunto el delito informático y han realizado charlas y capacitaciones para que puedan enfrentar este delito.

Millones Velásquez indica que la aparición y evolución de las tecnologías y herramientas informáticas en los últimos años son de gran ayuda para la humanidad. El hombre como ser evoluciona siendo este un claro ejemplo de su evolución. Sin embargo, este desarrollo ha permitido que la criminalidad avance burlando las medidas de seguridad adoptadas por las empresas que ofrecen el servicio de comercio electrónico, creando base de datos falsos cometiendo delitos informáticos. Por lo tanto, nace la persecución del Estado representado por el Ministerio Público. Rodríguez Flores menciona que perseguir los delitos contra el patrimonio, estafa agravada, artículo 196 A del Código Penal. Pedir información a los bancos, centros comerciales (datos consignados) sea virtual o físico.

Respecto a la pregunta: ¿Qué recomendaciones haría para que el Ministerio Público de Lima centro mejore su desempeño en la persecución del delito de fraude informático cometido a través del E-comerce en la lucha contra la ciberdelincuencia? Señalaron:

Cárdenas Moreno señala que como es conocido, el Ministerio Público en reciente data diciembre de 2020, ha creado la Unidad especializada en ciberdelincuencia y muy recientemente mediados o fines de 2021 ha creado las primeras fiscalías especializadas en ciberdelitos, una de ellas es la ubicada en Lima Centro, por tanto, mi recomendación como integrante también de la Red de Fiscales en Ciberdelincuencia del distrito Fiscal de Junín, es que se siga capacitando al personal fiscal y además al personal auxiliar así como adquirir las herramientas necesarias para el combate de esta nueva modalidad delictiva contar con softwares, peritos informáticos para obtener la evidencia digital será necesario para llevar a estos delincuentes al banquillo de los acusados, por otro lado, creo que las fiscalías de prevención deben de reorientar o adicionar a sus objetivos de prevención este tipo de delitos, concientizar a la población a través de los colegios,

profesores sobre el peligro existente y latente en el uso del INTERNET, evitando así los delitos más frecuentes, fraudes informáticos, *Sexting, Child Groming*, etc.

Mejia Izaguirre sostiene que se require: 1) aprovisionamiento de medios logísticos para la realización de pesquisas y pericias digitales forenses, tales como computadoras y dispositivos tecnológicos de última generación y de software forenses; 2) capacitación de los operadores jurídicos en ciencias y técnicas de informática, los cuales deben ser permanentes ante el avance constante de la tecnología informática.

Soca Rodríguez manifiesta que se de realizar: 1) capacitaciones a los despachos fiscales como a los fiscales provinciales, fiscales adjuntos y asistente en función fiscal sobre los concerniente en el modus operandi en el delito de fraude informático y realizar las diligencias de investigación; 2) adquisición de medios logísticos y software con la finalidad de tener herramientas para las pericias y pesquisas. Montalván Castañeda indica que se siga implementando de equipos tecnológicos, software y capacitación al personal fiscal en esta clase de modalidad delictiva.

Baquerizo Haro señala que de haber trabajo y reunión con el personal de DIVINDAT y elaborar planes de trabajo para elaborar planes de trabajo en conjunto. Bustamante indica que se solicite la medida limitativa de derecho, levantamiento del secreto de las comunicaciones, bancarias, indispensables en estos casos.

Espinoza Prado informa que trabajar en conjunto con las PNP a fin de obtener pruebas idóneas para que sustenten la acción penal. Larico Rodríguez manifiesta que poner énfasis en las solicitudes de información a los bancos a fin de que estos brinden información de manera casi inmediata. Tramitar y obtener resultados en las medidas limitativas del levantamiento del secreto de las comunicaciones y levantamiento del secreto bancario.

Millones Velásquez indica que mejorar los canales de capacitación a los operadores de justicia, en especial a la Policía y a los fiscales de turno como primeros responsables frente a hechos de ciberdelincuencia. Rodríguez Flores

menciona que actuar de manera urgente e inaplazable en las diligencias preliminares.

Respecto a la pregunta: Hay quienes sostienen que el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del E-comerce, resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021 ¿cuál es su posición al respecto? Señalaron:

Cárdenas Moreno señala que la creación de estas nuevas fiscalías especializadas es de reciente data, es obvio que los resultados no van hacer los esperados, la falta de experiencia, la falta de recursos logísticos, personal administrativo, técnicos informáticos, peritos informáticos, softwares especiales hacen que los investigadores (PNP, MP) no tengan los elementos necesarios ni siquiera para poder identificarlos e individualizarlos a estas personas tanto más que como es sabido en este tipo de delitos la evidencia digital es volátil es decir, desaparece fácilmente y si no se actúa de manera inmediata esta no va ser acopiada por otro lado, la obtención de las mismas no es de fácil acceso, es por eso la necesidad de nuestros operadores de este tipo de delitos estén debidamente capacitados de no ser así, los resultados nos serán ajenos a nuestros objetivos de lucha frontal contra este tipo delitos y esta exigencia debe ser para todo tipo de investigación la falta de recursos humanos logísticos, van incidir en los resultados, haciendo un parangón con el soldado que va a la guerra sin las armas adecuadas es evidente que va sucumbir ante el enemigo, por más preparado que esté, por eso creo que es necesario atender este problema.

Mejía Izaguirre sostiene que teniendo en cuenta que recién se han creado el Sistema de las fiscalías especializadas en ciberdelincuencia, considera que si bien se ha tenido la impresión que su función no ha sido satisfactoria, sin embargo, espero que conforme avance el tiempo y gracias a la praxis que vayan adquiriendo así como a la implementación de infraestructura, ,logística y personal que necesiten para cumplir con sus funciones se van a percibir mayores logros para combatir este tipo de delitos.

Soca Rodríguez manifiesta que son políticas de altos funcionarios o jerarquías que no implementan políticas contra la ciberdelincuencia y por eso recién se han creado las fiscalías especializadas en ciberdelincuencia. Los avances se verán a largo plazo hasta preparar a los fiscales en la lucha contra la ciberdelincuencia. Montalván Castañeda indica que como esta modalidad delictiva se ha incrementado hace muy poco tiempo, ha conllevado a que las instituciones públicas presenten cierta deficiencia.

Baquerizo Haro señala que al Ministerio Público le falta realizar mayor coordinación con el personal PNP especializado de DIVINDAT y así aunar ideas en la persecución de los delitos informáticos. Bustamante indica que se implemente con más equipos tecnológicos y que se obtenga información por la cooperación internacional.

Espinoza Prado informa que el rol principal del Ministerio Público en el delito de fraude informático sería coordinar con especialistas tanto de la PNP como del Ministerio Público para encontrar los indicios o evidencias digitales para la sustentación de la acción penal. Larico Rodríguez manifiesta que se debe a la falta de información proporcionada por las entidades, así también a que la ley no especifica el delito informático, hay varios vacíos legales que hacen que este delito en su mayoría quede impune. Millones Velásquez indica que totalmente de acuerdo. La falta de tecnología hace que la delincuencia a través de estos medios siga generando a la sociedad. Rodríguez Flores menciona que aún se encuentra en implementación.

Respecto al **Objetivo específico 1**: Evaluar el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021, se preguntó:

¿Cuál cree que fue el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

Cárdenas Moreno señala que la Oficina Técnica del Ministerio Público no tiene una relación directa con la salvaguarda del derecho al patrimonio en el delito de fraude informático, creo que la pregunta debe ser reformulada en la siguiente; Qué

acciones debe tener en cuenta la Oficina Técnica del Ministerio Público para la lucha frontal contra el Fraude Informático? dado que esta oficina es la que propone, implementa, monitorea paulatinamente los cambios necesarios para el adecuado funcionamiento de la unidad fiscal, así podríamos contestar la necesidad que esta oficina brinde mayor presupuesto para la contratación de peritos, capacitaciones del personal fiscal y auxiliar, entre otras para mejorar la lucha frontal en este tipo de delitos.

Mejia Izaguirre sostiene que el rol de la Oficina Técnica del Ministerio Público tiene por finalidad brindar apoyo técnico especializado a las investigaciones que realizan las fiscalías. En cuanto al fraude informático cuenta con la oficina de peritajes digitales forenses con la finalidad de realizar las pericias e informes correspondientes que se requieran. Soca Rodríguez manifiesta que la Oficina Técnica del Ministerio Público tiene por finalidad brindar apoyo técnico especializado a las investigaciones que realizan las fiscalías en cuanto al fraude informático cuenta con la Oficina de peritajes digitales forenses que realizan los informes periciales correspondientes.

Montalván Castañeda indica que no tiene conocimiento que se haya implementado una Oficina técnica del Ministerio Público en salvaguarda del derecho al patrimonio por delito informático. Baquerizo Haro señala que se debe coordinar y unificar criterios con el laboratorio informático de la DIVINDAT y sustentar el recojo de las evidencias digitales para sustentar la acción penal. Bustamante indica que con charlas preventivas a través de publicaciones escritas y habladas. Espinoza Prado informa que unificar ideas con el laboratorio informático de la PNP para sustentar el recojo de las evidencias digitales para la sustentación de la acción penal.

Larico Rodríguez manifiesta que charlas preventivas, coordinación constante con la PNP, para orientar a la ciudadanía y puedan evitar e identificar los delitos informáticos. Millones Velásquez indica que crear fuentes que ayuden a mitigar los avances de los delitos cometidos por los medios electrónicos. Rodríguez

Flores menciona que la elaboración de análisis y pericias a los equipos tecnológicos vinculados a un delito informático.

Respecto a la pregunta: ¿De qué manera la Oficina Técnica del Ministerio Público podría mejorar su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático? Mencionaron:

Cárdenas Moreno señala que la Oficina Técnica del MP, no tiene dentro de sus objetivos la salvaguarda de los derechos patrimoniales de las víctimas del fraude informático, sino sus objetivos es diseñar, proponer, implementar, fortalecer, las unidades fiscales para la lucha frontal contra todo tipo de delitos evidentemente, al ser los ciberdelitos un campo por decirlo así en nuestro derecho penal nuevo existe una necesidad apremiante para dotarles de las herramientas necesarias para la lucha optima de no ser así, lamentablemente seguiremos teniendo los resultados en negativo, pero por otro lado téngase en cuenta que estas fiscalías en Ciberdelincuencia de Lima Centro, son fiscalías nuevas y que creo que evaluarlas sobre sus logros no sería la adecuada, hay que dejarlas trabajar.

Mejia Izaguirre sostiene que considerando que el accionar delictivo en esta clase de eventos ilícitos se materializan a través del manejo de datos informáticos, los cuales pueden ser volátiles y desaparecer de los soportes en los cuales se encuentran registrados. Es necesario que la Oficina Técnica del Ministerio Público cumpla con sus funciones con la diligencia y celeridad del caso.

Soca Rodríguez manifiesta que una opción para mejorar el desempeño sería contratar más personal experto en ciberdelincuencia y fraude informático, capacitación y tener personal preparado que puedan cumplir su rol. Montalván Castañeda indica que desconoce. Baquerizo Haro señala que se debe unificar ideas con el laboratorio informático de la PNP. Bustamante indica que a través de publicaciones o los medios televisivos o de fuentes abiertas: Facebook o Instagram. Espinoza Prado informa que coordinación con el laboratorio informático de la PNP. Larico Rodríguez manifiesta que falta una fluida comunicación con el personal PNP que investiga los delitos informáticos. Millones Velásquez indica que fortalecer la

capacitación a las personas y la colectividad. Rodríguez Flores menciona que la implementación de equipos es primordial.

Respecto a la pregunta: Hay quienes señalan que el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó limitado ya que no contó con implementos tecnológicos y logística especializada que le permitió llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos en el periodo 2021 ¿cuál es su posición al respecto? Mencionaron:

Cárdenas Moreno señala que la Unidad Especializada en ciberdelincuencia se encuentra trabajando y a la fecha creo que está teniendo el apoyo de la Oficina Técnica del Ministerio Público si no fuera así no tendríamos creadas estas fiscalías provinciales especializadas ya en Lima, siendo estas a casi un poco más de un año de creada esta unidad, reitero hay que dejarlas trabajar, no olvidemos que Roma no se construyó en un día. Mejia Izaguirre sostiene que la problemática no surge por la carencia de implementos tecnológicos o logísticos, sino por la gran demanda y cantidad de pericias e informes que se les solicita realizar, lo cual podría subsanarse con la contratación de más personal.

Soca Rodríguez manifiesta que podría entenderse que la carga que maneja la Oficina Técnica del Ministerio Público le genera una gran demanda y cantidad de pericias e informes, lo cual se puede solucionar contratando más personal. Montalván Castañeda indica que efectivamente al ser una modalidad delictiva reciente, que surgió con más énfasis a raíz del estado de emergencia en Perú, el Ministerio Público no se encuentra preparado tanto en personal fiscal y logístico para realizar estas investigaciones con eficacia.

Baquerizo Haro señala que no hubo mucha capacitación con el personal especializado hacia el personal del laboratorio de la PNP. Bustamante indica que falta mayor énfasis en la severidad de las leyes. Espinoza Prado informa que cuando no se tiene los medios tecnológicos y logísticos especializados, cualquier oficina técnica o laboratorio de la PNP no resulta eficiente. Larico Rodríguez manifiesta que reestructuración de la norma, falta de datos de las empresas.

Millones Velásquez indica que efectivamente, se desconoce el procedimiento. La aplicación de las herramientas a seguir. Tener en cuenta que este tipo de delitos se produce desde un ordenador que muchas veces no domicilia en Perú. Rodríguez Flores menciona que siempre habrá comentarios, pero el compromiso y el abastecimiento de equipos es necesario para una óptima resolución de las investigaciones.

Respecto al Objetivo **específico 2**: Evaluar la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el fraude informático en el periodo 2021, se plantearon las preguntas:

¿Cuál fue la labor que desarrolló la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

Cárdenas Moreno señala que el trabajo que, realizada toda división o sección de investigación de la PNP, es la de coadyuvar a lucha frontal de todo tipo de delitos, en este caso la División de la DIVIDAT de la PNP, es justamente combatir este tipo de delitos informático como es el fraude informático y así salvaguardar el derecho patrimonial de sus víctimas no del delito. Mejia Izaguirre sostiene que la DIVINDAT como estamento policial especializado le compete a poyar la investigación que lleva a cabo la fiscalía en los delitos informáticos. Soca Rodríguez manifiesta que el rol de la DIVINDAT es apoyar en las investigaciones de los despachos ya que cuentan con el aparato logístico y el personal.

Montalván Castañeda indica que tiene conocimiento que en la sede Lima sí se cuenta con la logística adecuada que permita que muchos casos sean resueltos de forma eficiente y en un tiempo récord. Baquerizo Haro señala que se debe perseguir los delitos informáticos y todas sus modalidades. Bustamante indica que es llegar al público a través de los medios de comunicación, darle una orientación adecuada del uso de los medios tecnológicos y aplicaciones. Espinoza Prado informa que perseguir los delitos enmarcado en la ley de delitos informáticos Ley 30096 y su modificatoria.

Larico Rodríguez manifiesta que charlas preventivas, conferencias, atención al público con la finalidad de hacerles conocer las modalidades del delito informático. Millones Velásquez indica que están iniciando este tipo de labores ya que es un delito poco perseguido por la justicia. Rodríguez Flores menciona que investigador el delito cometido.

Respecto a la pregunta: ¿Qué recomendaciones haría para que la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional mejore su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático? Mencionaron:

Cárdenas Moreno señala que más que una recomendación lo que tendría que hacer es brindarle mi reconocimiento al trabajo que vienen realizando, solicitando no desfallecer dado que no es fácil investigar este tipo de delitos y que no olvidemos que la PNP y MP, son las instituciones que deben estar siempre coordinadas para la lucha frontal con este tipo de delitos. Mejia Izaguirre sostiene que se debe: 1) asimilar a ingenieros en ciencias informáticas a efectos de que participen de forma directa con las investigaciones que se realizan en esta clase de delitos, 2) implementar la oficina de peritajes con material logístico y de software necesarios para dicha labor.

Soca Rodríguez manifiesta que se debe capacitar al personal PNP DIVINDAT y contratar personal de procedencia civil como ingenieros informáticos, así como crear escuelas o cursos especializados para mejorar las investigaciones académicamente y así tener buenos cuadros en la PNP. Montalván Castañeda indica que se capacite al personal policial que labora en Comisarías ya que son ellos los que toman conocimiento de forma inicial del delito y que el tiempo que transcurre es importante en esta clase de delincuencia para que se resuelva de forma exitosa.

Baquerizo Haro señala que debe realizarse capacitación internacional permanente e implementarlo con la logística adecuada. Bustamante indica que incremento de personal, capacitaciones, implementación de equipos tecnológicos.

Espinoza Prado informa que una preparación constante en los delitos informáticos ya que la tecnología avanza y los delincuentes informáticos también se modernizan en sus modalidades. Larico Rodríguez manifiesta que una mejora en la adquisición de equipos tecnológicos, software licenciados y actualizados. Millones Velásquez indica que capacitar al personal policial dedicados a la persecución de este tipo de ilícitos. A la fecha esta capacitación es débil. Faltan capacitadores idóneos. Rodríguez Flores menciona que equipos tecnológicos.

Respecto a la pregunta: ¿Qué acciones significativas y exitosas han realizado las entidades competentes para proteger el derecho al patrimonio en el delito de fraude informático? Mencionaron:

Cárdenas Moreno señala que el trabajo es constante, y esto creo que se evidencia con las últimas acciones en donde se ha visto como recientemente se ha desbaratado toda una red de delincuentes cibernéticos dedicada a la clonación de tarjetas de créditos, otra una Banda que intento estafar a cadena de boticas en Tarapoto a través de la modalidad de Phishing.

Mejia Izaguirre sostiene que la acción más significativa en el ámbito del Ministerio Público es la creación de Fiscalías especializadas en ciberdelincuencias. Soca Rodríguez manifiesta que fue la creación de las Fiscalías especializadas en ciberdelincuencia. Montalván Castañeda indica que la difusión de formas preventivas para que los ciudadanos puedan cuidar su dinero, la creación de claves seguras, restricción de compras por internet, entre otros. Baquerizo Haro señala que realizar reuniones con el Ministerio Público, empresas bancarias, entidades móviles, etc. Bustamante indica que publicidad para evitar brindar información secreta referida a cuentas de ahorros o crédito.

Espinoza Prado informa que orientación a la sociedad sobre los delitos informáticos, patrullaje virtual constante en la internet. Larico Rodríguez manifiesta que publicidad advirtiéndole a los ciudadanos que no brinden información personal ni contraseñas. Millones Velásquez indica que no se conoce a la fecha, son pocos los logros conocidos por los medios televisivos. Rodríguez Flores menciona que publicidad preventiva.

Respecto a la pregunta: Hay quienes señalan que la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó deficiente ya que no contó con personal calificado, logística y recursos que le permitan llevar a cabo operativos de prevención e intervención en estos delitos en el periodo 2021 ¿cuál es su posición al respecto? Mencionaron:

Cárdenas Moreno señala que esta apreciación de esta unidad policial es errónea, dado al desconocimiento que se tiene de este tipo de delitos, su complejidad hace que muchas veces demore los resultados solamente con una trabajo constante y objetivo es que se puedan desbaratar estas bandas lo cual se viene obteniendo resultados a pesar de los escasos recursos que se cuenta.

Mejia Izaguirre sostiene que en efecto, la carencia de personal capacitado, medios logísticos (tanto de hardware como software) han imposibilitado que dicha división especializada cumpla sus funciones con eficacia. Soca Rodríguez manifiesta que eso ocurre porque los funcionarios de alta jerarquía de la PNP no contratan personal de procedencia civil capacitado. Es un tema de gestión pública. No realizan adquisiciones de software originales. No existe inversión en software.

Montalván Castañeda indica que esta es una realidad delictiva que se está dando hace poco tiempo y como es de suceder las instituciones no se encontraban preparadas para que exista un avance en las investigaciones. Baquerizo Haro señala que las necesidades son constantes, pero el personal que labora en DIVINDAT da su mejor trabajo para la lucha contra la ciberdelincuencia. Bustamante indica que falta mayor severidad en las penas.

Espinoza Prado informa que la necesidad de recursos y personal calificado y logístico es constante pero la fortaleza que tiene la DIVINDAT es su personal. Gracias a ellos se realizan operativos y la prevención. Larico Rodríguez manifiesta que sí falta un mayor incremento de personal técnico logístico, así también un cambio en las leyes. Millones Velásquez indica que totalmente de acuerdo. Debería ser la unidad policial la que deba contar con los mejores equipos y los mejores

investigadores en el rubro. Rodríguez Flores menciona que sí se requiere mayor personal, logística, etc., que facilite el proceso de investigación.

Respecto a la pregunta: ¿Algo más que dese agregar / comentarios / sugerencias?

Cárdenas Moreno señala que es una realidad la falta de profesionales ligados a este rubro que es la ciberdelincuencia es un campo nuevo en donde se requiere profesionales altamente capacitados, es por ello que felicito al tesista sobre el tema escogido, que nos brinda la oportunidad para señalar, que esta nueva forma de vida digital que se está posicionando en la vida de cada uno de nosotros así como nos ha traído facilidades también traen amenazas y debemos estar preparados para evitarlos y combatirlos.

Soca Rodríguez manifiesta que es un buen tema de investigación. Espera que se publique en revistas jurídicas para crear conciencia en los funcionarios de las Fiscalías y de la PNP, que de modo coordinado deben combatir la ciberdelincuencia. Baquerizo Haro señala que fortalecer y unificar ideas entre el Ministerio Público y la PNP y preparación constante en temas de delitos informáticos. Espinoza Prado informa que fortalecer la unificación de ideas entre la PNP y el Ministerio Público, preparación constante en los delitos informáticos. Rodríguez Flores menciona que para la persecución de este delito es recomendable la constante capacitación de las personas que se encargan de las investigaciones.

Análisis de la técnica de la entrevista: como se aprecia de las entrevistas a los Fiscales Provinciales, efectivos policiales, defensor público y abogados, todos están preocupados de la magnitud y de la gravedad del delito informático, el cual cada día se expande y utiliza nuevos mecanismos para llevarlo a cabo. Esto implica un enorme desafío para la administración de justicia, sobre todo, con los encargados de llevar a cabo las investigaciones: Ministerio Público y Policía Nacional, pues se requiere de ellos mayor profesionalismo, estrategias coordinadas y equipamiento adecuado.

De otro lado, los entrevistados señalan que la normativa existente para combatir este delito, requiere ser más explícita, más preventiva y más rígida en su

sanción, pues si estos delitos siguen quedando en la impunidad, este fenómeno se agravará aún más. En ese sentido, los entrevistados señalan que los operadores de justicia requieren contar con los recursos legales, logística necesaria y el personal calificado para combatir el delito informático de modo más efectivo y estratégico.

4.2. Descripción de resultados de la técnica del análisis de fuente documental: Doctrina y teorías

A continuación, se consignan los datos obtenidos de la técnica de análisis de fuente documental, tomando en cuenta los objetivos propuestos en la investigación.

Ya en 1994, y luego de la aparición y el uso masivo de la internet diversos penalistas reunidos en el XV Congreso Internacional de Derecho Penal, en Río de Janeiro – Brasil, señalaron como recomendación que la comunidad académica y científica, conjuntamente con los Estados deben comprometerse a desarrollar más estudios sobre el delito informático. La teoría y política pública debe estudiar y desarrollar leyes informáticas, considerando las cualidades específicas de la data, al compararla con los objetos tangibles y estudiar los posibles cambios que afectan los principios generales y modelos del Derecho Penal.

Al respecto creemos que Perú no tomó en cuenta en su momento las mencionadas recomendaciones a pesar que en 1994 ya se hacía masivo el uso de la internet en los hogares peruanos. Es así que recién luego de 2010 en que ha desarrollado una legislación específica para combatir el ciberdelito. Si bien al inicio de los años 90 este tipo de modalidad delictiva no era tan frecuente, consideramos que se debieron tomar acciones preventivas a fin de que no se expandiera del modo en que actualmente actúa. Es por ello, que creemos que el Estado a través del Derecho Penal y de los operadores del Derecho deben asumir acciones más proactivas y preventivas que permita combatir este delito.

Otra acción importante del Estado para combatir el ciberdelito fue la creación del Observatorio de criminalidad de la Fiscalía, instancia que tenía por objetivos hacer seguimiento a la evolución y desarrollo de los delitos en sus diversas modalidades, lugares y actores. Es así que, respecto a los delitos informáticos,

dicho Observatorio señala que desde el 2000 se han ido incrementando este tipo de ilícitos y que al cabo de 10 años se ha pasado de 24 casos a 223 casos reportados de ciberdelitos, lo que evidencia un aumento exponencial de los mismos, y que por ello mismo requería mayor acción por parte de los operadores del Derecho.

Tabla 4
Índice de los delitos informáticos entre 2000-2010

Ilícito	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010
Delitos Informáticos	24	26	29	44	57	81	81	109	112	189	223

Fuente: Observatorio de criminalidad del Ministerio Público (2011).

Por su lado, la División de investigación de delitos de alta tecnología de la PNP, señaló que entre el 2006 y el 2013 los delitos en las que utilizaban las TIC habían aumentado de manera considerable, haciendo cada vez más que las autoridades competentes de investigar y sancionar se quedarán siempre rezagados respecto al crimen. Los delincuentes cibernéticos sofisticaban cada vez más su modo de proceder, se especializaban haciendo uso de redes informáticas, uso de software y hardware que les permite intervenir la información cibernética de las personas.

El aumento de los delitos informáticos se detalla a continuación.

Tabla 5
Delitos con uso de las tecnologías de la información y comunicación, 2006-2013

Delito	2006	2007	2008	2009	2010	2011	2012	2013	TOTAL
Delitos Informáticos	77	73	128	125	161	184	147	85	980
Pornografía Infantil	53	72	43	65	90	151	136	49	659
Hurtos de Fondo	93	200	239	523	384	705	401	126	2671
Otros	53	58	53	223	299	468	184	242	1580
Total	276	403	463	936	934	1508	868	502	5890

Fuente: División de investigación de delitos de alta tecnología de la Policía Nacional del Perú (2014).

Como se aprecia de la tabla, cada vez más los delitos cibernéticos se diversifican y se hacen más complejos y especializados. Es así que aparecen ahora la pornografía infantil, el hurto de fondos, estafa electrónica, entre otras modalidades en que se usas las tecnologías de la información y comunicación para cometer actos ilícitos. Siendo así los bienes jurídicos afectados también se diversifican. Ya no solo es el derecho al patrimonio, la intimidad, sino además la libertad sexual, la indemnidad, el honor y la integridad física, emocional y psicológica.

4.3. Descripción de resultados de la técnica: Análisis normativo

En el Código Penal peruano (1991) ya estaba el delito de hurto virtual en el artículo 186, el cual lo castigaba con cárcel no menor de 3 ni mayor de 6 años y con 180 a 365 días-multa, cuando el agente utilizaba sistemas de transferencia electrónica de fondos, de la internet o violaba las claves secretas. Luego, mediante Ley 26319 (1994) la sanción se aumentó a cárcel no menor de 4 ni mayor de 8 años, manteniéndose sin modificación sustancial alguna hasta que fue derogada por Ley 30096 (2013).

No obstante, esas iniciativas legales de los años 90 y 2000, el legislador peruano consideró que solo sancionaba un limitado número de ilícitos penales, dejando en la impunidad muchas otras modalidades delictivas en los que se empleaban mecanismos informáticos. Es por ello que el Parlamento consideró de plantear y aprobar una nueva política criminal relacionada a los delitos informáticos que incluía nuevas figuras penales: turismo sexual, pornografía infantil, fraude electrónico, apología al terrorismo, entre otros.

Luego de amplios debates y de contar con mayor información y casuística, en el 2000 los congresistas aprueban la Ley 27309 que creó el delito informático, incorporando el artículo 207-A al Código Penal, el Delito de alteración, daño y destrucción de base de datos, sistema, red o programa de computadoras, incorporando el artículo 207-B 13 al Código Penal y el delito informático agravado, incorporando el artículo 207-C al Código Penal.

No obstante, estos avances normativos, la situación de aquel entonces nos lleva a precisar y analizar algunas cuestiones, que son remarcadas por Elías (2004):

a) El legislador asumió la criminalidad cibernética solo con el fraude digital, por lo que su tipificación se limitó en el Título V del Código Penal - sección de delitos contra el patrimonio. Esto se debió a que al inicio se pensaba que estos ilícitos eran sólo una ampliación de lo que el Código Penal de 1991 preveía como agravantes en el hurto (utilización de sistemas de transferencia electrónicas de fondos, de la internet o la violación de las claves secretas). Por ello, muchos autores han señalado que estos delitos no forman parte del Derecho Penal Económico ni protegen la seguridad informática o la intimidad pues identifican al patrimonio como el principal –o, en algunos casos, como el único– bien jurídico protegido por estas normas.
b) Al ser asumidos como ilícitos contra el patrimonio, de modo equivocado fueron asumidos como delitos de peligro y no de resultado. Es por ello que, en el debate previo a su aprobación, se señaló que el delito de peligro surge ya desde el ingreso del uso indebido de los medios informáticos o a la data de las personas implicadas en los mismos o en las bases de datos, sea para sabotear, espiar, defraudar o dañar. Es decir, no se necesita que se produzca un resultado para estar frente a un delito informático, basta con la intención. Sin embargo, el Artículo IV del Código Penal prevé que la sanción, necesariamente, precisa de la lesión o puesta en peligro de derechos protegidos por la ley, de ahí que existan delitos de resultado y delitos de peligro concreto y abstracto. Cuando el legislador identificó este nuevo tipo de delitos como ilícitos contra el patrimonio, creó una paradoja. Ya que, si esto fuese así, el ingreso a la base de datos no debió ser sancionada ya que no afectaba o ponía en riesgo el patrimonio de la persona. Luego de un amplio debate y análisis, el legislador asumió que se debía reconocer que el bien jurídico no era solo el patrimonio sino una gama distinta de derechos informáticos, debiéndose crear un Título independiente en el Código Penal para su adecuada legislación.

c) El legislador usó las sanciones penales como *prima ratio* así evitó acudir a una instancia administrativa que sancione acciones que por su gravedad (cuantitativa o cualitativa) no merezcan el máximo reproche punitivo estatal. Además, promulgó la norma sin contar con personal técnico especializado que colaborase con las investigaciones preliminares o judiciales, lo que originó que muchos procesos quedaran impunes.
d) Luego de la incorporación de estos delitos al Código Penal, diversos legisladores planteaban aumentar los castigos, crear otras modalidades delictivas, mejorar la redacción de los tipos penales siguiendo los lineamientos internacionales que cada vez se desarrollaban o mejoraban las unidades especiales a cargo de su investigación y juzgamiento.
e) Durante los siguientes años a la incorporación de los delitos informáticos al Código Penal, el número de estas acciones ilícitas aumentaron. Así, entre enero de 2000 y diciembre de 2010, se registraron 975 denuncias en 27 distritos judiciales, pero sólo se formalizaron el 32.3% de estas.

En 2013 se aprueba el delito de tráfico Ilegal de datos, incorporando el artículo 207-D al Código Penal, al Capítulo de Delitos Informáticos mediante la Ley 30096. Esta ley aprobada con el propósito de combatir la inseguridad ciudadana, razón por la cual se cambiaron 28 artículos del Código Penal y se crearon 3 delitos, entre ellos el tráfico ilegal de datos pues el legislador consideró que uno de los problemas relacionados a la inseguridad ciudadana se ligaba a la comercialización indebida de datos. Lamentablemente, la redacción de esta norma era ambigua que podía castigarse incluso las acciones desarrolladas por las agencias de medios o publicidad a través de las *mailing list.*

Siendo así, la normativa penal empezó a considerar la sanción de ilícitos haciendo uso de las Tecnologías de la información y Comunicación, quedando un nuevo listado de delitos y que se detallan a continuación.

Tabla 6

Nuevos delitos informáticos incorporados en el Código Penal

Nuevos delitos informáticos	Descripción
Pornografía Infantil	Incorporado en el artículo 183-A aprobado el 26 de mayo de 2001, se creó el delito de pornografía infantil; sin embargo, mediante la Ley o. 28251 del 8 de junio de 2004, este ilícito fue modificado para precisar que la difusión a través del internet también es punible y así evitar lagunas legislativas que pudiesen generar cualquier tipo de impunidad.
Turismo Sexual Infantil	Incorporado en el artículo 181- A precisando que una de las modalidades a sancionar sería aquella en el que se emplee Internet para su promoción. He de precisar que la Ley 30096 individualizó el empleo de las tecnologías de la información o de la comunicación como un agravante.
Clonación o adulteración de terminales de telefonía celular	Incorporado en el artículo 222-A., mediante Ley 28774 del 2006 en respuesta al alto índice porcentual de hurtos de celulares registrado un año antes. Según el legislador, de 28,814 hurtos de menor cuantía, la Policía constató que 14,804 eran celulares (64.88%) los cuales –y en esto se fundamenta la creación de este tipo penal– serían utilizadas por los delincuentes para cometer otros actos delictivos como extorsión, secuestro y robo
Apología al delito de terrorismo	Incorporado en el artículo 316, modificado por el Decreto Legislativo 982 del 2007, el cual incorporó como circunstancia agravante la apología al terrorismo a través de los medios de comunicación, incrementándose de 12 a 15 años la pena máxima para este tipo de actividades. Según la Exposición de Motivos del referido Decreto Legislativo, la agravación de la pena se debería a la apología al terrorismo se viene difundiendo peligrosamente a través de Internet ya que "tienen un alcance ilimitado a nivel nacional e internacional."
Delito de atentado a la integridad de datos informáticos en las modalidades sugeridas en el Convenio de Budapest.	La norma peruana se aparta del Convenio de Budapest al asumir los términos "introduce" y "hace inaccesible" a la redacción del tipo penal. En efecto, al sancionarse otro tipo de conductas como "daña", "borra", "deteriora", "altera" o "suprime" –que sí fueron recomendadas por el Convenio– las incorporaciones de las dos modalidades en comentario se convierten en inadecuadas. En efecto, ¿cuándo debería castigarse penalmente la "introducción" de datos informáticos? La respuesta está vinculada a una carencia de la norma: cuando se produzcan daños graves. Nuestra norma actual no lo prevé por lo que no tiene sentido y, de hecho, atenta contra el principio de lesividad del Derecho Penal, pues dicha modalidad per se no ocasiona daño alguno. Asimismo, sostengo que el término "hace inaccesible" es inútil por cuanto es una consecuencia de la modalidad "daña".
Delito de atentado a la integridad de sistemas informáticos (sabotaje informático)	El artículo 3 del Convenio de Budapest sanciona el dañar, borrar, deteriorar, alterar o suprimir los datos informáticos, y el artículo 4 del Convenio de Budapest castiga la obstaculización grave del funcionamiento de un sistema informático o a través de la introducción o transmisión de datos informáticos. La redacción del Convenio es coherente; porque en esta regulación sí tiene sentido las modalidades de introducción y transmisión pues son el medio para la obstaculización grave del sistema información. Si bien una conducta podría originar la configuración de ambos tipos delictivos, lo cierto es que nos encontraríamos frente a un concurso aparente de delitos pues el especial absorbe al general. Lamentablemente la legislación peruana no siguió la formulación normativa del Convenio de Budapest

Delito de Proposiciones a niños, niñas y adolescentes con fines sexuales por medios tecnológicos	Este delito no forma de las recomendaciones del Convenio de Budapest, pero sí del Convenio del Consejo de Europa sobre la Protección de Niños contra la Explotación Sexual y el Abuso Sexual (2007). Según esta norma, es un acto delictivo contactar a un menor de 14 años para solicitar u obtener material pornográfico o para llevar a cabo actividades sexuales con él. La redacción nos permite afirmar que se sanciona el mero contacto, sin importar que se llegue a solicitar, obtener el material pornográfico o se lleven a cabo las actividades sexuales. De este modo, nuestro Legislador ha adelantado la barrera de punibilidad de manera peligrosa pues ha convertido el *child grooming* en un delito de peligro abstracto al no requerir un riesgo inminente.
Elusión de medidas tecnológicas, productos destinados a la elusión de medidas tecnológicas y servicios destinados a la elusión de medidas tecnológicas	Incorporado en el artículo 220- A, 220-B y 220-C mediante Ley 29263 del 2008 –modificada por la Ley 292316 del 2009- incorporó estas tres modalidades delictivas propuestas por el Poder Ejecutivo a fin de cumplir con las obligaciones asumidas por el Estado peruano en el artículo 16 del Acuerdo de Promoción Comercial Perú – Estados Unidos (APC).
Ingreso Indebido de equipos o sistemas de comunicación, fotografía y/o filmación en centros de detención o reclusión	Incorporado en el artículo 368-A y 368-B, mediante Ley 29867 del 2012 con la finalidad de combatir los crímenes cometidos o direccionados desde el interior de los centros penitenciarios. En este sentido, el legislador consideró que diversas herramientas electrónicas podrían ser empleadas para la comisión de nuevos delitos pues el espacio físico no era un impedimento para ello, por lo que no sólo prohibió su uso sino que creó tipos penales que castigan el ingreso indebido de estos.
Delito de Acceso Ilícito	En ella se sanciona el hacking blanco o mero intrusismo pues sólo se requiere el acceso ilícito a través de la vulneración de las medidas de seguridad para su configuración. De este modo, por ejemplo, si estudiantes de Ingeniería Informática quieren poner en práctica sus conocimientos y demostrar que pueden sobrepasar las medidas de seguridad de determinadas empresas para estudiar sus puntos vulnerables, no lo podrán hacer (sin autorización previa) pues estarían cometiendo un acto delictivo pese a que no persigan una finalidad ilícita adicional (lucrar con su actividad o causar algún tipo de perjuicio).

A estos delitos se agrega el de Tráfico ilegal de datos (Art. 154-A), el delito de interceptación de datos informáticos, el fraude informático y los delitos informáticos contra la fe pública. Como se aprecia, es amplia la normativa que penaliza los ilícitos en la que hacen uso de las TIC. A partir de lo expuesto, creemos que la experiencia casuística y los aportes de la doctrina y las teorías han permitido un desarrollo normativo importante en el país, han permitido su discusión, actualización y planteamientos de políticas criminales mucho más especializadas y estratégicas.

En este acápite también se presenta **la discusión de los resultados**, el cual se establece desde la interpretación de los resultados obtenidos a partir de la

temática estudiada por lo que conviene indicar que no es la repetición de los resultados, por lo contrario, es el análisis crítico y juicios de valor que le da sentido a los resultados. En este contexto Domínguez (2015) sostiene que la discusión sigue el orden de los principales resultados estableciendo de tal modo que facilite la toma de postura respecto de una teoría, un curso de acción o de un fenómeno. Para tal efecto, se plantea la discusión a partir de las convergencias y divergencias de la información obtenida.

Tabla 7
Triangulación de convergencias y divergencias de la información obtenida

Convergencias	Divergencias
Los entrevistados Cárdenas Moreno, Mejía Izaguirre, Soca Rodríguez, Montalván Castañeda, Baquerizo Haro, Bustamante Espinoza Prado, Larico Rodríguez, Millones Velásquez y Rodríguez Flores señalaron que la ciberdelincuencia es hoy en día uno de los más graves problemas sociales y penales. La sociedad y el Estado no han sido preparados para enfrentar este flagelo que cada vez se expande y se diversifica más	Algunos entrevistados (Millones Velásquez y Rodríguez Flores) señalan que las penas deben ser más severas para castigar la ciberdelincuencia pues su permisividad hace que estos delitos queden en la impunidad y eso no contribuye a combatirlo eficazmente. Desde el presente estudio creemos que, si bien las penas deben ser contundentes para sancionar el ciberdelito, lo que debería enfatizar más el Estado es en la prevención
Todos los entrevistados señalan que el Ministerio Público y la Policía deben contar con el personal calificado, los implementos, equipos, infraestructura y logística necesaria para enfrentar la ciberdelincuencia, caso contrario, esta seguirá en aumento.	Creemos que el gobierno central debe dotar al Ministerio Público y a la Policía de los medios necesarios para investigar y sancionar el delito. Los laboratorios donde se realizan las pesquisas y peritajes deben estar equipados e implementando de tal modo que puedan llevar a cabo su labor de la mejor manera.
La doctrina y los expertos entrevistados coinciden en señalar que actualmente se cuenta con una legislación que, si bien está permitiendo combatir la ciberdelincuencia de un modo más efectivo e integral, el problema y limitación sigue siendo la falta de recursos y logística de las entidades competentes.	El legislador al momento de aprobar la normativa sobre ciberdelincuencia no ha considerado el Derecho comparado y las experiencias de otros países para combatir la ciberdelincuencia. Desde los años 90 en que se emitieron normas sobre

	ciberdelincuencia, la legislación ha sido incoherente, limitada y no se ha contado con la participación de todos los implicados: bancos, empresas, expertos, juristas, usuarios. En ese sentido, creemos que el legislador debe abrir la discusión con los especialistas para que se cuente con una normativa mucho más completa y sistemática
La doctrina, sobre todo europea ha sido un referente al momento de legislar sobre ciberdelincuencia ya que en dicho continente la ciberdelincuencia apareció desde los años 80 y debido al uso masificado de los medios digitales de los ciudadanos, los delincuentes han utilizado con mayor audacia los medios cibernéticos para cometer diversos delitos. Estos datos también coinciden con los que posee el Observatorio de Criminalidad del Ministerio Público y la División de investigación de delitos de alta tecnología de la Policía Nacional del Perú.	Los entrevistados señalan de modo divergente que Perú no aprovechó adecuadamente la experiencia en ciberdelincuencia que ocurría en países europeos y en Estados Unidos. Aquí todavía se esperó a que ese fenómeno ocurra para recién legislar y sancionar, mientras tanto muchas personas que fueron afectadas en su patrimonio, dignidad u honor, no fueron resarcidas por falta de una normativa y preparación de las autoridades competentes para intervenir en la problemática
Desde la doctrina, Acosta (2003, Elías (2014) y Espinoza (2017) coinciden en señalar que el ciberdelito es hoy en día el mayor desafío para la administración de justicia y para los operadores del Derecho. Tanto jueces, fiscales y policías requieren estar mejor preparados para enfrentar un fenómeno que muchas veces es difícil de rastrearlo, identificar y sancionarlo.	Algunos entrevistados no conocen plenamente la normativa penal sobre ciberdelincuencia. Para ello, todavía se trata de un tema relativamente nuevo, pero que reconocen que es necesario informarse y capacitarse
La Organización Mundial del Comercio (1998), Morales (2016) y Mengoa (2021) coinciden en señalar que el ciberdelito es un asunto de seguridad pública mundial, pues no solo atañe a un solo país o continente, sino a todo el planeta. Los ciberdelincuentes pueden estar cometiendo el delito de un país a otros y eso implica que debe existir tratados y convenios internacionales que les permita	A diferencia de la experiencia planteada por la Organización Mundial del Comercio, Morales y Mengoa, los entrevistados para este estudio no han señalado la importancia de actuar legalmente de modo más interactivo entre un país y otro. Creemos que el legislador y el operador del Derecho peruano debe asumir que la ciberdelincuencia no tiene límites

a los Estados combatirlo de modo integral e interinstitucional	geográficos o políticos, sino que se trata de un fenómeno mundial y así debe ser entendido.
Todos los entrevistados han coincidido en que al cabo de los años el Perú ya cuenta con una legislación contra la ciberdelincuencia y que esta se ha ido actualizando con el devenir de los años y de la casuística, y que los operadores del Derecho, actualmente se encuentran más capacitados que antes. Ya nadie niega la realidad que el mundo y el país luego de la pandemia de la COVID19 ha cambiado para siempre	Creemos que los operadores del Derecho deben participar de modo permanente en Congreso Internacionales de Derecho Penal para que mantengan activos y actualizados sus conocimientos y aprendan de otras experiencias, tanto teóricas como prácticas. Es decir, no se puede actuar o vivir de espaldas del desarrollo tecnológico del mundo, más por el contrario, se trata de estar en constante actualización y capacitación

V. CONCLUSIONES

1. El Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-comerce*, ha demostrado que no estuvo capacitado ni contó con la logística, personal idóneo y los equipos necesarios que le permitan investigar, obtener pruebas, peritajes e indicios para llevar a cabo su labor, por lo que este resultó poco significativo y lo que es más grave, este tipo de delitos ha quedado impune.

2. La Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático no ha contado con los medios necesarios que le permitan cumplir su labor. Los equipos e implementos con los que cuenta no son de última generación ni tecnología de punta; la logística que posee no es tan especializada es por ello que no le ha permitido llevar a cabo una correcta y adecuada investigación e identificar a los ciberdelincuentes que cometieron estos ilícitos. Esto se ha debido a una falta de decisión política institucional por fortalecer dicha Oficina Técnica.

3. La División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático ha desarrollado una experiencia empírica importante lo que le ha permitido enfrentar y llevar a cabo operativos de prevención e intervención en estos delitos, a pesar de las limitaciones de falta de personal calificado, logística y recursos.

4. El uso cada vez más masificado y diversificado de las tecnologías de la información y comunicación, de las redes sociales, aplicativos y la internet ha permitido que la ciberdelincuencia sea cada vez más sofisticada en su accionar. Ello ha conllevado a que los legisladores y los operadores del Derecho actualicen la normativa y el modo de proceder para combatir este tipo de delitos que se expande incluso de un país a otro.

VI. RECOMENDACIONES

El Ministerio Público de Lima centro debe asumir una política institucional que permita fortalecer su actuación en la persecución del delito de fraude informático cometido a través del E-comerce, ello implica dotar de infraestructura, logística y contratar personal especializado e idóneo que le permita luchar contra el flagelo de la ciberdelincuencia.

La Oficina Técnica del Ministerio Público debe poseer mayor autonomía administrativa, logística y económica que le permita salvaguardar el derecho al patrimonio en el delito de fraude informático, de este modo superar sus limitaciones de implementos tecnológicos y logísticos especializados. Dicha Oficina deberá actuar de modo interinstitucional y transectorial a todo el Ministerio público y las demás entidades públicas y privadas competentes para llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos.

La División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional del Perú debe asumir una política institucional que le permita contar con presupuesto y medios para contratar personal calificado, adquirir logística y recursos especializados que le permitan salvaguardar el derecho al patrimonio en el delito de fraude informático. En ese sentido, le corresponderá al Ministerio del Interior solicitar al Ministerio de Economía el presupuesto necesario.

División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional del Perú y el Ministerio Público deben implementar planes y programas dirigidos a la prevención del delito de fraude informático y el ciberdelito en general. Ello implicará desarrollar programas educativos e informativos masivos para que la población sepa de modo preciso la manera cómo debe utilizar los medios que ofrece las tecnologías de la información y comunicación. Muchos recursos y tiempo ahorrarían el Estado si es que asumen políticas criminales mucho más preventivas.

REFERENCIAS

Acosta, A. (2003). *Hacking, cracking y otras conductas ilícitas cometidas a través de internet*. Universidad de Chile. Recuperado de Asturias. Corporación Universitaria (2018). Introducción al E-Commerce. España. Recuperado de https://bit.ly/3r7aOzL.

BBC Mundo (2017). Un nuevo ciberataque de gran escala afecta a compañías e instituciones de todo el mundo. Recuperado de https://bbc.in/3jfifQV.

Bernal, C., (2010). *Metodología de la investigación*. (3ª ed.). Bogotá: PEARSON Educación.

Carrasco, S. (2007). *Metodología de la investigación científica*.

Convenio de Budapest o Convenio sobre la Ciberdelincuencia aprobado el 2001.

Convenio del Consejo de Europa sobre la Protección de Niños contra la Explotación Sexual y el Abuso Sexual (2007).

DW (2017). Hecho en Alemania - Industria 4.0: tecnología versus tradición. *DW Español*. Recuperado de https://bit.ly/3JclBPi.

Elías, R. (2014). Luces y sombras en la lucha contra la delincuencia informática en el Perú. Lima: Hiperderecho.

Espinoza, M. (2017). Derecho Penal Informático: deslegitimación del poder punitivo en la sociedad de control. Tesis. Universidad Nacional del Altiplano. Facultad de Ciencias Jurídicas y Políticas. Puno.

Espinoza, M. (2014). Los delitos informáticos en el Perú: Panóptico del poder punitivo. Editorial: *Taripaña*.

Garcés, H. (2000). *Investigación Científica*. Quito: Ediciones Abya-Yala

Gutiérrez, D. (2018). La razón del éxito del E-comerce. Versión electrónica. Mundo ejecutivo. Recuperado de https://bit.ly/3LJr8i5.

Hall, A. (2010). Tipos de delitos informáticos. Recuperado de https://bit.ly/3JdGCJF.

Hernández, R., Fernández, C. y Baptista, P. (2014). *Metodología de la Investigación.* (6ta ed.). México: Mc Graw Hill.

Iglesias, J. (2018) titulado El impacto del comercio electrónico en los emprendedores de diseño de la ciudad autónoma de Buenos Aires. Trabajo de investigación final. Universidad Argentina de la Empresa. Recuperado de https://bit.ly/3KdiDvb.

Infobae. (2017). Ciberataque mundial impacta a instituciones estatales y privadas en una dimensión nunca antes vista. Buenos Aires. Recuperado de https://bit.ly/3JhSxpv.

Ley 26319 (1994).

Ley 30096 (2013).

Mengoa, M. (2021). Punibilidad del comportamiento del *phisher-mule* en el delito de fraude informático en el Perú. Tesis para optar el título de abogada. Universidad César Vallejo. Recuperado de https://bit.ly/3ucheja.

Morales, D. (2016). La inseguridad al utilizar los servicios de redes sociales y la problemática judicial para regular los delitos informáticos en el Perú-2015. Tesis para optar el título profesional de abogado. Universidad Señor de Sipán. Recuperado de https://bit.ly/35JbbJt.

Observatorio de criminalidad del Ministerio Público (2011). Lima.

Organización Mundial del Comercio (1998). *E-comerce.* Consejo General de la Organización Mundial del Comercio.

Price Wáter House Cooper. *Global Economic Survey (2014)*. Recuperado de https://pwc.to/3J6i9G0

Principios Internacionales de Derechos Humanos sobre Vigilancia de las Comunicaciones.

Recomendaciones del XV Congreso Internacional de Derecho Penal. Sección II – Sobre delitos informáticos y otros delitos cometidos contra la tecnología informática. Evento realizado entre el 4 y 10 de setiembre de 1994 en Río de Janeiro - Brasil. Recomendación N° 24.

Téllez, J. (2008). *Derecho informático* (4 ed.). México: McGraw-Hill Interamericana.

Urbano, S. (2017). Ventajas y desventajas del comercio electrónico. Actualidad E-comerce. Recuperado en abril del 2018 en https://bit.ly/3NSewXA.

Villavicencio, F. (2015). Delitos informáticos en la Ley 30096 y La modificación de la ley 30071. *Revista virtual del Centro de Estudios en Derecho Penal*. Recuperado de https://bit.ly/3Kgag1U.

Zaffaroni, E. (2009). *Estructura básica del derecho penal*. Buenos Aires, Argentina: Ediar.

ANEXOS

Anexo 3: Validación de instrumentos

UNIVERSIDAD CÉSAR VALLEJO

SOLICITO:

Validación de instrumento de recojo de información.

Sr.: Julio Cesar VALLES ROJAS

Yo, **César Jonathan VERÁSTEGUI QUINTANILLA,** identificado con DNI Nº 43450202 alumno de la Escuela Profesional de Derecho, a usted con el debido respeto me presento y le manifiesto:

Que siendo requisito indispensable el recojo de datos necesarios para la tesis que vengo elaborando titulada: **El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce.* 2021**, solicito a Ud. Se sirva validar el instrumento que le adjunto bajo los criterios académicos correspondientes. Para este efecto adjunto los siguientes documentos:

- Instrumento
- Ficha de evaluación
- Matriz de consistencia

Por tanto:

A usted, ruego acceder mi petición.

Lima, 1 de marzo de 2022.

.....

César Jonathan VERÁSTEGUI QUINTANILLA

FIRMA

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Rojas Julio Cesar

1.2. Cargo e institución donde labora: Divincri PNP

1.3. Nombre del instrumento motivo de evaluación: Ficha de entrevista

1.4. Autor de Instrumento: Cesar Jonathan VERASTEGUI QUINTANILLA.

II. ASPECTOS DE VALIDACIÓN

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

III. OPINIÓN DE APLICABILIDAD

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

IV. PROMEDIO DE VALORACIÓN :

95 %

Lima, 27 enero del 2022.

FIRMA DEL EXPERTO INFORMANTE

DNI No. 40353277 Telf.: 993561105

UNIVERSIDAD CÉSAR VALLEJO

SOLICITO:

Validación de instrumento de recojo de información.

Sr.: Jefferson Williams GUERRA CAMPOS

Yo, **César Jonathan VERÁSTEGUI QUINTANILLA,** identificado con DNI N° 43450202 alumno de la Escuela Profesional de Derecho, a usted con el debido respeto me presento y le manifiesto:

Que siendo requisito indispensable el recojo de datos necesarios para la tesis que vengo elaborando titulada: **El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce.* 2021**, solicito a Ud. Se sirva validar el instrumento que le adjunto bajo los criterios académicos correspondientes. Para este efecto adjunto los siguientes documentos:

- Instrumento
- Ficha de evaluación
- Matriz de consistencia

Por tanto:

A usted, ruego acceder mi petición.

Lima, 1 de marzo de 2022.

.....

César Jonathan VERÁSTEGUI QUINTANILLA
FIRMA

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

1.1. Apellidos y Nombres: Guerra Campos, Jefferson Williams

1.2. Cargo e institución donde labora: Docente de la UCV

1.3. Nombre del instrumento motivo de evaluación: Ficha de entrevista

1.4. Autor de Instrumento: César Jonathan VERÁSTEGUI QUINTANILLA.

II. ASPECTOS DE VALIDACIÓN

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

III. OPINIÓN DE APLICABILIDAD

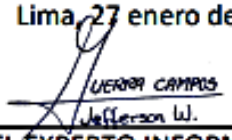
- El Instrumento cumple con los Requisitos para su aplicación
- El Instrumento no cumple con Los requisitos para su aplicación

X

IV. PROMEDIO DE VALORACIÓN :

90 %

Lima, 27 enero del 2022.



FIRMA DEL EXPERTO INFORMANTE

DNI No. 71012547 Telf.: 993533611

Anexo 3: Validación de instrumentos

UNIVERSIDAD CÉSAR VALLEJO

SOLICITO:

Validación de instrumento de recojo de información.

Sr.: Marco Antonio ANTEQUERA TINOCO

Yo, **César Jonathan VERÁSTEGUI QUINTANILLA,** identificado con DNI Nº 43450202 alumno de la Escuela Profesional de Derecho, a usted con el debido respeto me presento y le manifiesto:

Que siendo requisito indispensable el recojo de datos necesarios para la tesis que vengo elaborando titulada: **El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce.* 2021**, solicito a Ud. Se sirva validar el instrumento que le adjunto bajo los criterios académicos correspondientes. Para este efecto adjunto los siguientes documentos:

- Instrumento
- Ficha de evaluación
- Matriz de consistencia

Por tanto:

A usted, ruego acceder mi petición.

Lima, 1 de marzo de 2022.

.....

César Jonathan VERÁSTEGUI QUINTANILLA

FIRMA

UNIVERSIDAD CÉSAR VALLEJO

VALIDACIÓN DE INSTRUMENTO

I. **DATOS GENERALES**

1.1. Apellidos y Nombres: Antequera tinoco Marco Antonio

1.2. Cargo e institución donde labora: Jefe del Departamento de Altos Dirrehum

1.3. Nombre del instrumento motivo de evaluación: Ficha de entrevista

1.4. Autor de Instrumento: César Jonathan VERÁSTEGUI QUINTANILLA.

II. **ASPECTOS DE VALIDACIÓN**

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

III. OPINIÓN DE APLICABILIDAD

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

IV. PROMEDIO DE VALORACIÓN :

96 %

Lima, 27 enero del 2022.

FIRMA DEL EXPERTO INFORMANTE

DNI No. 31651925 Telf.: 979093336

GUÍA DE ENTREVISTA

Dirigido a expertos en ciberdelito / policías / fiscales

TÍTULO: El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce*. 2021

Entrevistado: Luis Alvaro Cardenas Moreno

Cargo / grado académico Abogado

Institución donde labora: Ministerio Público

OBJETIVO GENERAL

Determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia en el periodo 2021

1. ¿En qué consiste el fraude informático cometido a través del *E-commerce*?

En palabras sencillas, podría señalar que el fraude informático cometido a través del E- comerce no es nada nada mas ni nada menos que la estafa cometido en el mundo del comercio electrónico . Como es sabido el desarrollo de la tecnología como el internet asi como las nuevas tercnologías de la información y comincaición (TICs) han hecho que nuestras vidas se conviertan en una vida mas virtualizada, es así que el mundo del comercio no ha sido ajena a ello razón de la existencia de "e-commerce" comercio electrónico que ha permitido que muchas empresas pequeñas y grandes hayan podido realizar sus actividades comerciales a través del mundo electrónico tanto más en tiempos de pandemia en donde el distanciamiento social era imprescindible para la subsitencia de la vida humana; sin embargo, esta nueva vida comercial a traido consigo riesgos y ataques en sus sistemas operativos no solo a las empresas que la utilizan sino también a los propios consumidores a través de este tipo de estafas cibernéticas, en donde una vez obtenidas sus datos informáticos registradas en dicha plataforma virtual, proceden a desviar tus fondos con o sin el consetimiento del titular, apropiándose así de manera ilegítima de su patrimonio.

2. ¿Cuál fue el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

El papel, que juega el MP, asi como en los otros delitos comunes es la lucha contra esta y la prevención de la misma,

y esta persecución penal frente a esta modalñidad delictiv esta regulada a través de la Ley 30096 y su posterior modificación Ley N° 30171, que tiene por fianlidad combatir los delitos informáticos o ciberdelitos, en el caso puntual que estamos tocando el fraude informático está regulado en el artículo 8° de esta ley, que señala: "El que deliberadamente procura para asi o para otro unprovecho ilícito mediante el diseño, introducción (...) de datos informáticos o cualquier interferencia o manipulación en el funcionamiento informático, será (...) la modalidad mas frecuente en este medio "comercio electrónico" es el que se manifesta a través del conocido "phishing" en donde el ciberdelincuente lo que hace es obtener los datos informáticos registrados e dicha plataforma para luego de ello haciendo un uso ilegítimo del mismo apropiarse de su patrimonio económico de sus victimas.

3. ¿Qué recomendaciones haría para que el Ministerio Público de Lima centro mejore su desempeño en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

Como es conocido, el Ministerio Público en reciente data diciembre de 2020, ha creado la Unidad especializada en ciberdelincuencia y muy recientemente medidados o fines de 2021 a creado las primeras fiscalias especializadas en ciberdelitos, una de ellas es la ubicada en Lima Centro, por tanto mi recomendación como integrante tambien de la Red de Fiscales en Ciberdelincuencia del distrito Fiscal de Junín, es que se siga capacitando al personal fiscal y además al personal auxilia así como adquerir las herramientas necesarias para el combate de esta nueva modalidad delictiva contar con sofwares, peritos informáticos para obtener la evidencia digital será necesario para llevar a estos delincuentes al banquillo de los acusados, por otro lado, creo que las fiscalias de preve deben de reorientar o adicionar a sus objetivos de prevención este tipo de delitos, concientizar a la pobl a través de los colegios, profesores sobre el peligro existente y latente en el uso del INTERNET, evitanc así los delitos mas frecuentes, fraudes informáticos, Sexting, Child Groming, etc.

Escriba el texto aquí

4. Hay quienes sostienen que el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce,* resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021 ¿cuál es su posición al respecto?

Como indique, líneas arriba la creación de estas nuevas fiscalias especializadas es de reciente data, es obvio que los resultados no van hacer los esperados, la falta de experienza, la falta de recursos logistricos, persional administrativo, tecnicos informáticos, peritos informáticos, sofwares especiales hacen que los investigadores (PNP, MP) no tengan los elementos necesarios ni siquiera para poder indentificarlos e individualizarlos a estas personas tanto mas que como es sabido en este tipo de delitos la evidencia digital es volatil es decir, desaparece facilmente y si no se actua de manera inmediasta esta no va ser acopiada por otro lado, la obtención de las mismas no es de facil acceso, es por eso la necesidad de nuestros operadores de este tipo de delitos esten debidamente capacitados de no ser así, los resultados nos seran ajenos a nuestros objetivos de lucha frontal contra este tipo delitos y esta exigencia debe ser para todo tipo de investigación la falta de recursos humanos logisticos, van incidir en los resultados, haciendo un parangon con el soldado que va a la guerra sin las armas adecuadas es evidente que va sucumbir ante el enemigo, por mas preparado que esté, por eso creo que es necesario atender este problema.

OBJETIVO ESPECÍFICO 1

Evaluar el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

5. ¿Cuál cree que fue el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

En realidad creo que la Oficina Tecnica del Ministerio Público no tiene una relación directa con la salvaguarda del derecho al patrimonio en el delito de fraude informático, creo que la pregunta debe ser reformulada en la siguiente; Qué acciones debe tener en cuenta la Oficina Técnica del Ministerio Público para la lucha frontal contra el Fraude Informático? dado que esta oficina es la que propone, implementa, monitorea paulatinamente los cambios necesarios para el adecuado funcionamiento de la unidad fiscal, asi podríamos contestar la necesidad que esta oficina brinde mayor presupuesto para la contratación de peritos, capacitaciones del personal fiscal y auxiliar, entre otras para mejorar la lucha frontal en este tipo de delitos.

6. ¿De qué manera la Oficina Técnica del Ministerio Público podría mejorar su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

Creo que esta pregunta ya ha sido contestada con la anteiror, en realidad debo ser claro, La Oficina Tecnica del MP, no tiene dentro de sus obtetivos la salvaguarda de los derechos que felicito al tesista sobre el tuste la patrimoniales de las víctmas del fraude informático, sino sus objetivos es diseñar, proponer, implementar, fortalecer, las unidades fiscales para la lucha frontal contra todo tipo de delitos evidentemente, al ser los ciberdelitos un campo por decirlo así en nuestro derecho penal nuevo existe una necesidad apremiamte para dotarles de las herramientas necesarias para la lucha optima de no ser asi, lamentablemente seguiremos teniendo los resultados en negativo, pero por otro lado téngase en cuenta que estas fiscalias en Ciberdelincuencia de Lima Centro, son fiscalias nuevas y que creo que evaluarlas sobre sus logros no sería la adecuada, hay que dejarlas trabajar.

7. Hay quienes señalan que el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó limitado ya que no contó con implementos tecnológicos y logística especializada que le permitió llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos en el periodo 2021 ¿cuál es su posición al respecto?

Reitero mi punto de vista señalada en las respuestas anteriores, la Unidad Especialziada en ciberdelincuecnia se encuentra trabajando y a la fecha creo que está teniendo el apoyo de la Oficina Técnica del Ministeiro Público sino fuera así no tendríamos creadas estas fiscalias provinles especialiadas ya en Lima, siendo estas a casi un poco mas de un año de creada esta unidad, reitero hay que dejarlas trabajar, no olvidemos que Roma no se cosntruyó en un día.

OBJETIVO ESPECÍFICO 2

Evaluar la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

8. ¿Cuál fue la labor que desarrolló la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

El trabajo que realizada toda división o sección de investigación de la PNP, es la de coadyuvar a lucha frontal de todo tipo de delitos, en este caso la División de la

DIVIDAT de la PNP, es justamente combatir este tipo de delitos informático como es el fraude informático y asi salvaguardar el derecho patrimonial de sus victimas no del delito, ojo.

9. ¿Qué recomendaciones haría para que la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional mejore su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

mas que una recomendación lo que tendría que hacer es brindarle mi reconocimiento al trabajo que vienen realizando, solicitando no desfallecer dado que no es facil investigar este tipo de delitos y que no olvidemos que la PNP y MP, son las instituciones que deben estar simepre coordinandas para la lucha frontal con este tipo de delitos.

10. ¿Qué acciones significativas y exitosas han realizado las entidades competentes para proteger el derecho al patrimonio en el delito de fraude informático?

El trabajo es constante, y esto creo que se evidencia con los últimos acciones en donde se ha visto como recientemente se ha desbaratado toda una red de delincuentes cibernéticos dedicada a la clonación de tarjetas de créditos, otra una Banda que intento estafar a cadena de boticas en Tarapoto a través de la modalidad de Phishing.

11. Hay quienes señalan que la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó deficiente ya que no contó con personal calificado, logística y recursos que le permitan llevar a cabo operativos de prevención e intervención en estos delitos en el periodo 2021 ¿cuál es su posición al respecto?

Considero, que esta apreciación de esta unidad policial es erronea, dado al desconocimiento que se tiene de este tipo de delitos, su complejidad hace que muchas veces demore los resultados solamente con una trabajo constante y objetivo es que se puedan desbaratar estas bandas lo cual se viene opteniendo resultados a pesar de los escasos recursos que se cuenta.

12. ¿Algo más que dese agregar / comentarios / sugerencias?

Es una realidad la falta de profesionales ligados a este rubo que es la ciberdelincuencia es un campo nuevo en donde se requiere profesionales altamente capacitados, es por ello que felicito al tesista sobre el tema escogido, que nos brinda la oportunidad para señalar que esta nueva forma de vida digiital que se esta posicionando en la vida de cada uno de nosotros así como nos ha traido facilidades también traen amenazas y debemos estar preparados para evitarlos y combatirlos. gracias.

SELLO del entrevistado	FIRMA del entrevistado
Luis Alvaro Cardenas Moreno FISCAL PROVINCIAL (P) Sexta Fiscalia Provincial Penal Corporativa - Huancayo Ministerio Publico - Distrito Fiscal Junin	Firma Digital Firmado digitalmente por CARDENAS MORENO Luis Alvaro FAU 20131370301 soft Motivo: Soy el autor del documento Fecha: 29.03.2022 05:54:58 -05:00

GUÍA DE ENTREVISTA

Dirigido a expertos en ciberdelito / policías / fiscales

TÍTULO: El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce*. 2021

Entrevistado: LUIS MEGIA IZAGUIRRE

Cargo / grado académico FISCAL ADJUNTO PROVINCIAL

Institución donde labora: MINISTERIO PUBLICO

OBJETIVO GENERAL

Determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia en el periodo 2021

1. ¿En qué consiste el fraude informático cometido a través del *E-commerce*?

CONSISTE EN LA DISTORSION, ALTERACION, SUPRESION O SUSTITUCIÓN DE DATOS INFORMATICOS CON LA FINALIDAD DE OBTENER UN PROVECHO ILICITO EN PERJUICIO DE TERCEROS EN LA REALIZACION DE ACTIVIDADES O TRANSACCIONES COMERCIALES A TRAVES DE INTERNET, APLICACIONES DE CELULARES Y CANALES INFORMATICOS (COMERCIO ELECTRONICO), ENTRE LOS CUALES TENEMOS LOS FRAUDES DE CLONACIÓN DE TARJETAS, TRANSFERENCIAS ELECTRONICAS FRAUDULENTAS, PHISING (ROBO DE IDENTIDAD) ETC.

2. ¿Cuál fue el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

POR MANDATO CONSTITUCIONAL AL MINISTERIO PUBLICO LE CORRESPONDE DIRIGIR LA INVESTIGACION DEL DELITO CON EL APOYO DE LA POLICIA -

NACIONAL. CON RESPECTO AL FRAUDE INFORMÁTICO EN EL COMERCIO ELECTRÓNICO EL MINISTERIO PÚBLICO HA CREADO LAS FISCALÍAS ESPECIALIZADAS EN CIBERDELINCUENCIA CON LA FINALIDAD DE COMBATIR CON MAYOR EFICACIA ESTE TIPO DE DELITOS.

3. ¿Qué recomendaciones haría para que el Ministerio Público de Lima centro mejore su desempeño en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

- APROVISIONAMIENTO DE MEDIOS LOGÍSTICOS PARA LA REALIZACIÓN DE PESQUISAS Y PERICIAS DIGITALES FORENSES, TALES COMO COMPUTADORAS Y DISPOSITIVOS TECNOLÓGICOS DE ÚLTIMA GENERACIÓN Y DE SOFTWARES FORENSES.
- CAPACITACIÓN DE LOS OPERADORES JURÍDICOS EN CIENCIAS Y TÉCNICAS DE LA INFORMÁTICA, LAS CUALES DEBEN SER PERMANENTES ANTE EL AVANCE CONSTANTE DE LA TECNOLOGÍA INFORMÁTICA.

4. Hay quienes sostienen que el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce*, resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021 ¿cuál es su posición al respecto?

TENIENDO EN CUENTA QUE RECIÉN SE HA CREADO EL SISTEMA DE LAS FISCALÍAS ESPECIALIZADAS EN CIBERDELINCUENCIA, CONSIDERO QUE SI BIEN SE HA TENIDO LA IMPRESIÓN QUE SU FUNCIÓN NO HA SIDO SATISFACTORIA. SIN EMBARGO ESPERO QUE

conforme avanza el tiempo y ganen la praxis que vayan adquiriendo, así como la implementación de infraestructura, logística y personal que requieran para el cumplimiento de sus funciones, se van a percibir mayores logros en combatir este tipo de delitos.

OBJETIVO ESPECÍFICO 1

Evaluar el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

5. ¿Cuál cree que fue el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

El rol de la Oficina Técnica del Ministerio Público tiene por finalidad brindar apoyo técnico especializado a las investigaciones que realizan las Fiscalías. En cuanto al fraude informático cuenta con la Oficina de Peritajes Digitales Forenses con la finalidad de realizar las pericias e informes correspondientes que se requieran.

6. ¿De qué manera la Oficina Técnica del Ministerio Público podría mejorar su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

Considerando que el accionar delictivo en esta clase de eventos ilícitos se materializan a través del manejo de datos informáticos, los cuales pueden ser volátiles y desaparecer de los soportes en los cuales se encuentran registrados, es necesario que la oficina técnica del Ministerio público cumpla

CON SUS FUNCIONES CON LA DILIGENCIA Y ECUNIDAD DEL CASO.

7. Hay quienes señalan que el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó limitado ya que no contó con implementos tecnológicos y logística especializada que le permitió llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos en el periodo 2021 ¿cuál es su posición al respecto?

CONSIDERO QUE LA PROBLEMATICA NO SURGE POR LA CARENCIA DE IMPLEMENTOS TECNOLOGICOS Y LOGISTICOS, SINO POR LA GRAN DEMANDA Y CANTIDAD DE PERICIAS E INFORMES QUE SE LES SOLICITAN REALIZAR, LO CUAL PODRÍA SUBSANARSE CON LA CONTRATACION DE MAS PERSONAL.

OBJETIVO ESPECÍFICO 2

Evaluar la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

8. ¿Cuál fue la labor que desarrolló la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

LA DIVINDAT COMO ESTAMENTO POLICIAL ESPECIALIZADO LE COMPETE APOYAR A LA INVESTIGACIÓN QUE LLEVA A CABO EL MINISTERIO PUBLICO EN LOS DELITOS INFORMATICOS.

9. ¿Qué recomendaciones haría para que la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional mejore su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

- ASIMILAR A INGENIEROS EN CIENCIAS INFORMATICAS A EFECTOS DE QUE PARTICIPEN EN

FORMA DIRECTA EN LAS INVESTIGACIONES QUE SE REALIZAN EN ESTA CLASE DE DELITOS. ASI COMO IMPLEMENTAR LA OFICINA DE PERITAJE CON MATERIAL LOGISTICO Y DE SOFTWARE NECESARIOS PARA DICHA LABOR.

10. ¿Qué acciones significativas y exitosas han realizado las entidades competentes para proteger el derecho al patrimonio en el delito de fraude informático?

CONSIDERO QUE LA ACCION MAS SIGNIFICATIVA EN EL AMBITO DEL MINISTERIO PUBLICO ES LA CREACION DE LAS FISCALIAS ESPECIALIZADAS EN CIBERDELINCUENCIA.

11. Hay quienes señalan que la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó deficiente ya que no contó con personal calificado, logística y recursos que le permitan llevar a cabo operativos de prevención e intervención en estos delitos en el periodo 2021 ¿cuál es su posición al respecto?

EFECTIVAMENTE, LA CARENCIA DE PERSONAL CAPACITADO, DE MEDIOS LOGISTICOS (TANTO DE HARDWARE COMO SOFTWARE) HAN IMPOSIBILITADO QUE DICHA DIVISION ESPECIALIZADA CUMPLA SUS FUNCIONES CON EFICACIA.

12. ¿Algo más que dese agregar / comentarios / sugerencias?

SELLO del entrevistado	FIRMA del entrevistado
LUIS HUMBERTO MEJIA AGUIRRE Fiscal Adjunto Provincial de la Fiscalía Corporativa Especializada en Delitos de Trata de Personas	

GUÍA DE ENTREVISTA

Dirigido a expertos en ciberdelito / policías / fiscales

TÍTULO: El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce*. 2021
Entrevistado: LUIS GABRIEL SOCA RODRIGUEZ
Cargo / grado académico: DEFENSOR PUBLICO - MINJUSDH - ABOGADO.
Institución donde labora: DIRECCION GENERAL DE DEFENSA PUBLICA DE LIMA ESTE - MINJUSDH

OBJETIVO GENERAL

Determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia en el periodo 2021

1. ¿En qué consiste el fraude informático cometido a través del *E-commerce*?

Consiste en la supresión, alteración, distorsión o sustitución de datos informaticos con la finalidad de obtener un provecho o ventaja ilícita en agravio de terceros, siendo el campo de acción de este flagelo en la realización de actividades o transacciones comerciales a través de internet, aplicaciones de programas de teléfonos celulares en el comercio electrónico, por ejemplo: clonación de tarjetas de crédito, transferencias electrónicas fraudulentas y robo de identidad (phising) entre otros.

2. ¿Cuál fue el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

El Ministerio Público es el persecutor del delito, es decir inicia y formaliza la investigación penal por mandato constitucional y mediante su ley orgánica, para estos delitos informáticos tiene como apoyo a las Unidades Especiales en ciberdelitos de la PNP con la finalidad de luchar contra la ciberdelincuencia que está avanzando a pasos agigantados.

3. ¿Qué recomendaciones haría para que el Ministerio Público de Lima centro mejore su desempeño en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

- Capacitaciones a los integrantes de los despachos fiscales, como los fiscales provinciales, fiscales adjuntos y asistentes función fiscal sobre lo concerniente en el modus operandi del delito de fraude informático y poder realizar las diligencias de investigación.

- Adquisición de Medios logísticos y software: con la finalidad de tener herramientas para las pericias o pesquizas

4. Hay quienes sostienen que el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce*, resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021 ¿cuál es su posición al respecto?

Son políticas de los encargados o funcionarios de esta jerarquía que no crean políticas contra la ciberdelincuencia, y en consecuencia recien se ha creado el sistema de las fiscalías especializadas en ciberdelincuencia, los avances se verán a largo plazo hasta poder preparar a los fiscales contra la lucha de la ciberdelincuencia.

OBJETIVO ESPECÍFICO 1

Evaluar el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

5. ¿Cuál cree que fue el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

La Oficina Tecnica del Ministerio Publico tiene por finalidad brindar apoyo tecnico especializado a los investigaciones que realizan los fiscales ; en cuanto al fraude informatico cuenta con la Oficina de peritajes digitales forenses para realizar los informes periciales correspondientes.

6. ¿De qué manera la Oficina Técnica del Ministerio Público podría mejorar su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

Una opción para mejorar el desempeño sería contar con más personal experto en cibercriminalidad y fraude informático, capacitados y con una unidad preparada para que puedan cumplir su rol.

7. Hay quienes señalan que el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó limitado ya que no contó con implementos tecnológicos y logística especializada que le permitió llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos en el periodo 2021 ¿cuál es su posición al respecto?

Podría catalogarse por la carga que maneja la Oficina Técnica del Ministerio Público, esto genera una gran demanda y cantidad de pericias e informes lo cual puede solucionarse contratando más personal.

OBJETIVO ESPECÍFICO 2

Evaluar la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

8. ¿Cuál fue la labor que desarrolló la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

El rol o labor de la DIVINDAT es apoyar en las investigaciones a los despachos fiscales, ya que cuentan con apoyo logístico y personal.

.....

.....

9. ¿Qué recomendaciones haría para que la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional mejore su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

Capacitar al personal PNP - DIVINDAT y contratar personal de procedencia civil como ingeniero informáticos, así como crear escuelas o curso especializados para mejorar a los investigadores académicamente y así tener buenos cuadros en la PNP.

10. ¿Qué acciones significativas y exitosas han realizado las entidades competentes para proteger el derecho al patrimonio en el delito de fraude informático?

Considero que la creación de Fiscalías Especializadas en Ciberdelincuencia

11. Hay quienes señalan que la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó deficiente ya que no contó con personal calificado, logística y recursos que le permitan llevar a cabo operativos de prevención e intervención en estos delitos en el periodo 2021 ¿cuál es su posición al respecto?

Eso ocurre porque los funcionarios de Alta Jerarquía de la PNP no contratan personal de procedencia civil capacitado, ya que en temas de Gestión Pública, no realizar adquisiciones de software originales, no existe inversión en software.

12. ¿Algo más que desee agregar / comentarios / sugerencias?

Es una buena forma de investigación, siempre que se aplique en nuestro ámbito jurídico para poder coordinar con las funciones que tienen la Fiscalía y PNP que entiendo que la unión hace un binomio de investigación y solo así se luchará contra la delincuencia.

SELLO del entrevistado	FIRMA del entrevistado
LUIS GABRIEL SOCA RODRIGUEZ DEFENSOR PUBLICO DE LIMA ESTE DIRECCION GENERAL DE DEFENSA PUBLICA DEL MINISTERIO DE JUSTICIA-DDHH.	

GUÍA DE ENTREVISTA

Dirigido a expertos en ciberdelito / policías / fiscales

TÍTULO: El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce*, 2021
Entrevistado: Kathya Montalvan Castañeda
Cargo / grado académico: Fiscal Adjunto Provincial.
Institución donde labora: Ministerio Público

OBJETIVO GENERAL

Determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia en el periodo 2021

1. ¿En qué consiste el fraude informático cometido a través del *E-commerce*?

Los fraudes informatico denominado "E-commerce" son las clonaciones de tarjeta, transferencias electrónicas fraudulenta, compras por internet mediante información de tarjeta de crédito o débito.

2. ¿Cuál fue el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

Considero que se debe de haber basado en la implementación de logística y capacitación del personal fiscal en esta clase de delitos.

3. ¿Qué recomendaciones haría para que el Ministerio Público de Lima centro mejore su desempeño en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

Sigue implementando de equipos tecnológico, Sofware y capacitación al personal fiscal en esta clase y modalidad delictiva.

4. Hay quienes sostienen que el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce*, resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021 ¿cuál es su posición al respecto?

Como esta modalidad delictiva se ha incrementado hace muy poco tiempo, ha conllevado a que las instituciones públicas presenten cierta deficiencia.

OBJETIVO ESPECÍFICO 1

Evaluar el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

5. ¿Cuál cree que fue el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

No tengo conocimiento que se halla implementado una oficina técnica del Ministerio Público en salvaguarda del derecho al patrimonio en el delito de fraude informático.

6. ¿De qué manera la Oficina Técnica del Ministerio Público podría mejorar su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

Desconozco.

7. Hay quienes señalan que el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó limitado ya que no contó con implementos tecnológicos y logística especializada que le permitió llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos en el periodo 2021 ¿cuál es su posición al respecto?

Efectivamente al ser una modalidad delicta reciente, que surgio con mas enfasis a raiz del Estado de Emergencia en el Perú, el Ministerio Publico no se encontro preparado tanto en personal fiscal y logistico para poder realizar estas investigaciones con eficacia.

OBJETIVO ESPECÍFICO 2

Evaluar la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

8. ¿Cuál fue la labor que desarrolló la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

Tengo conocimiento que en la Sede Lima, si se cuenta con la logistica adecuada que permitió que muchos

casos sean resueltos de forma eficiente y en un tiempo record.

9. ¿Qué recomendaciones haría para que la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional mejore su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

Que se capacite al personal policial que labora en comisarías, ya que son ellos quienes toman conocimiento de forma inicial del delito, y que el tiempo que transcurre es importante en este clase de delincuencia para que se resuelva de forma exitosa

10. ¿Qué acciones significativas y exitosas han realizado las entidades competentes para proteger el derecho al patrimonio en el delito de fraude informático?

La difusion de formas preventivas para que los ciudadanos puedan cuidar su dinero, como la edoccación de claves seguras, restricción de compras por internet, entre otros.

11. Hay quienes señalan que la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó deficiente ya que no contó con personal calificado, logística y recursos que le permitan llevar a cabo operativos de prevención e intervención en estos delitos en el periodo 2021 ¿cuál es su posición al respecto?

Como explique lineas arriba, este es una modalidad delictiva que se esta dando hace poco tiempo y como es de suceder las instituciones no se encontraban preparadas pero que existe un avance en las investigaciones.

12. ¿Algo más que dese agregar / comentarios / sugerencias?

.....

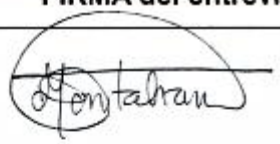
Ninguno.

.....

.....

.....

.....

SELLO del entrevistado	FIRMA del entrevistado
Kattya Monzalvin Castañeda FISCAL ADJUNTA PROVINCIAL(P) Quinta Fiscalía Provincial Penal Corporativa Huancayo Ministerio Público Distrito Fiscal Junín	

GUÍA DE ENTREVISTA

Dirigido a expertos en ciberdelito / policías / fiscales

TÍTULO: El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce*. 2021

Entrevistado: JOSE LUIS BAÑUELOZIZO HARO

Cargo / grado académico SI PNP / TECNICO SUPERIOR

Institución donde labora: PNP

OBJETIVO GENERAL

Determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia en el periodo 2021

1. ¿En qué consiste el fraude informático cometido a través del *E-commerce*?

CONSISTE EN LOS FRAUDES INFORMÁTICOS QUE SE EFECTUAN AL REALIZAR COMPRAS Y VENTAS DE PRODUCTO O SERVICIOS ATRAVEZ DEL INTERNET COMO REDES SOCIALES, EN SU MAYORIA ESTAS MODALIDADES SE OBSERVAN CON MAYOR FRECUENCIA EN LA RED SOCIAL DE FACEBOOK Y EN LA PÁGINA DE INTERNET MERCADOLIBRE.

2. ¿Cuál fue el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

TRABAJAR EN FORMA CONJUNTA CON LA POLICIA NACIONAL DEL PERU (DIVISIÓN DE INVESTIGACIÓN DE DELITOS INFORMÁTICOS) EN LAS INVESTIGACIONES POR FRAUDE INFORMÁTICO.

3. ¿Qué recomendaciones haría para que el Ministerio Público de Lima centro mejore su desempeño en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

TRABAJO Y REUNION CON PERSONAL DE DIVINDAT Y ELABORAR PLAN DE TRABAJO PARA MEJORAR EL TRABAJO EN CONJUNTO.

4. Hay quienes sostienen que el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce*, resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021 ¿cuál es su posición al respecto?

- EL ROL DEL MINISTERIO PÚBLICO, LE FALTO REALIZAR MAYOR COORDINACION CON EL PERSONAL PNP ESPECIALIZADO DE DIVINDAT Y ASI PODER UNAR IDEAS EN LA PERSECUCION DEL DELITO DE FRAUDE INFORMÁTICO.

OBJETIVO ESPECÍFICO 1

Evaluar el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

5. ¿Cuál cree que fue el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

COORDINAR Y UNIFICAR CRITERIOS CON EL LABORATORIO INFORMATICO DE LA PNP - DIVINDAT, Y SUSTENTAR EL RECOJO DE LOS EQUIPOS DIGITALES PARA SUSTENTAR LA ACCIÓN PENAL.

6. ¿De qué manera la Oficina Técnica del Ministerio Público podría mejorar su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

COORDINAR Y UNIFICAR IDEAS CON EL LABORATORIO INFORMATICO DE LA PNP.

7. Hay quienes señalan que el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó limitado ya que no contó con implementos tecnológicos y logística especializada que le permitió llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos en el periodo 2021 ¿cuál es su posición al respecto?

EN PARTE NO HUBO MUCHA CAPACITACION DE SU PERSONAL, COMO AL PERSONAL CON EXPERIENCIA DEL LABORATORIO DE LA PNP. — — —

OBJETIVO ESPECÍFICO 2

Evaluar la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

8. ¿Cuál fue la labor que desarrolló la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

PERSEGUIR LOS DELITOR INFORMATICOS Y TODAS SUS MODALIDADES. — — — —

9. ¿Qué recomendaciones haría para que la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional mejore su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

CAPACITACIÓN INTERNACIONAL PERMANENTE Y IMPLEMENTAR CON LA LOGISTICA APROPIADA. —

10. ¿Qué acciones significativas y exitosas han realizado las entidades competentes para proteger el derecho al patrimonio en el delito de fraude informático?

- REUNIONES DE LAS ENTIDADES COMO EL M.P, COMPAÑIAS DE TELEFONIA MOBIL, EMPRESAS ENTIDADES BANCARIAS.

11. Hay quienes señalan que la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó deficiente ya que no contó con personal calificado, logística y recursos que le permitan llevar a cabo operativos de prevención e intervención en estos delitos en el periodo 2021 ¿cuál es su posición al respecto?

LAS NECESIDADES SON CONSTANTES, PERO EL PERSONAL QUE LABORA EN DIVINDAT DA SU MEJOR TRABAJO PARA LA LUCHA CONTRA LA CIBERDELINCUENCIA.

12. ¿Algo más que dese agregar / comentarios / sugerencias?

* FORTALECER Y UNIFICAR IDEAS CON EL M.P Y LA PNP.

* PREPARACION CONSTANTE EN TEMAS DE DELITOS INFORMATICOS.

SELLO del entrevistado	FIRMA del entrevistado
SA. 31489678 JOSE LUIS BAQUERIZO HARO S1 - PNP	

GUÍA DE ENTREVISTA

Dirigido a expertos en ciberdelito / policías / fiscales

TÍTULO: El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce*. 2021
Entrevistado: JOSE E.
Cargo / grado académico S3
Institución donde labora: DIVINDAT

OBJETIVO GENERAL

Determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia en el periodo 2021

1. ¿En qué consiste el fraude informático cometido a través del *E-commerce*?

Consiste en adquirir compras por internet de una plataforma con la finalidad de obtener un producto sin la intención de pagar su valor, para conseguir evitar el cargo.

2. ¿Cuál fue el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

Evaluar la conducta en base a lo determinado recibida por la unidad PNP o por el ministerio público

3. ¿Qué recomendaciones haría para que el Ministerio Público de Lima centro mejore su desempeño en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

- Que se robote la medida limitativa de derecho, levantamiento del secreto de las comunicaciones y bancaria, inobjetable en estos casos.

4. Hay quienes sostienen que el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce*, resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021 ¿cuál es su posición al respecto?

- Que se implemente con mas equipos tecnologicos, que se protege la informacion de cooperacion internacional.

OBJETIVO ESPECÍFICO 1

Evaluar el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

5. ¿Cuál cree que fue el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

- Por charlas preventivas a través de la publicidad escrita y hablada.

6. ¿De qué manera la Oficina Técnica del Ministerio Público podría mejorar su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

- A través de las publicidades por los medios televisivos ó de fuentes abiertas (FACEBOOK, INSTAGRAM.)

7. Hay quienes señalan que el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó limitado ya que no contó con implementos tecnológicos y logística especializada que le permitió llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos en el periodo 2021 ¿cuál es su posición al respecto?

Si, falta mayor esfuerzo en la observancia de las leyes

OBJETIVO ESPECÍFICO 2

Evaluar la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

8. ¿Cuál fue la labor que desarrolló la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

Da luces al público a través de los medios de televisión, dando una orientación adecuada del uso de los medios tecnológicos y Aplicaciones

9. ¿Qué recomendaciones haría para que la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional mejore su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

Incremento de personal capacitaciones, implementación de

equipos tecnológicos.

10. ¿Qué acciones significativas y exitosas han realizado las entidades competentes para proteger el derecho al patrimonio en el delito de fraude informático?

- publicados para que den dando información cuenta diaria, tarjetas de robo);

11. Hay quienes señalan que la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó deficiente ya que no contó con personal calificado, logística y recursos que le permitan llevar a cabo operativos de prevención e intervención en estos delitos en el periodo 2021 ¿cuál es su posición al respecto?

Si, ya que falta una capacitación en los peritos.

12. ¿Algo más que dese agregar / comentarios / sugerencias?

NO.

SELLO del entrevistado	FIRMA del entrevistado
J.E. Bustamante 2 3219004	

GUÍA DE ENTREVISTA

Dirigido a expertos en ciberdelito / policías / fiscales

TÍTULO: El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce*, 2021
Entrevistado: VICTOR ESPINOZA PRADO
Cargo / grado académico SS. PNP
Institución donde labora: DIVINDAT.

OBJETIVO GENERAL

Determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia en el periodo 2021

1. ¿En qué consiste el fraude informático cometido a través del *E-commerce*?

- CUANDO SE COMPRA CON TARJETA DE CREDITO Y/O DEBITO CLONADAS EN LA PAGINA WEB DE UNA TIENDA VIRTUAL.

- AL INGRESAR A LA PAGINA WEB DE LA TIENDA VIRTUAL Y MODIFICAR LA BASE DE DATO PARA REALIZAR COMPRAS FRAUDULENTA.

2. ¿Cuál fue el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

- EL ROL DEL MINISTERIO DEFENSOR DE LA LEGALIDAD Y ORIENTA PARA LA OBTENCION DE LAS PRUEBAS Y SE

LA LEGALIDAD PARA EL EJERCICIO OPORTUNO DE LA ACCION PENAL.

3. ¿Qué recomendaciones haría para que el Ministerio Público de Lima centro mejore su desempeño en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

- TRABAJAR EN CONJUNTO CON LA PNP A FIN ENCONTRAR PRUEBAS IDONIAS PARA QUE SUSTENTEN LA ACCION PENAL.

4. Hay quienes sostienen que el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce*, resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021 ¿cuál es su posición al respecto?

- EL ROL PRINCIPAL DE MINISTERIO PUBLICO EN EL DELITO DE FRAUDE INFORMATICO SERIA COORDINAR CON ESPECIALISTA TANTO DE LA PNP Y MP PARA ENCONTRAR LOS INDICIOS Y/O EVIDENCIA

DIGITAL PARA LA SUSTENTACION DE LA ACCION PENAL.

OBJETIVO ESPECÍFICO 1

Evaluar el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

5. ¿Cuál cree que fue el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

UNIFICAR IDEAS CON EL LABORATORIO INFORMATICO DE LA PNP, PARA SUSTENTAR EL RECOJO DE LAS EVIDENCIAS DIGITALES PARA LA SUSTENTACION DE LA ACCION PENAL.

6. ¿De qué manera la Oficina Técnica del Ministerio Público podría mejorar su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

COORDINACION CON LOS LABORATORIO INFORMATICO DE LA PNP.

.....

.....

7. Hay quienes señalan que el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó limitado ya que no contó con implementos tecnológicos y logística especializada que le permitió llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos en el periodo 2021 ¿cuál es su posición al respecto?

.....

CUANDO NO SE TIENE LOS MEDIOS TECNOLOGICO Y LOGISTICO ESPECIALIZADO CUALQUIER OFICINA TECNICO Y/O LABORATORIO DE LA PNP, NO RESULTA EFICIENTE.

OBJETIVO ESPECÍFICO 2

Evaluar la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

8. ¿Cuál fue la labor que desarrolló la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

.....

PERSEGUIR LOS DELITOS ENMARCADO EN LA LEY DELITOS INFORMATICO LEY N°. 30096 Y SU MODIFICATORIA

.....

9. ¿Qué recomendaciones haría para que la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional mejore su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

.....

UNA PREPARACION CONSTANTE EN LOS DELITOS INFORMATICOS, YA QUE LAS

TECNOLOGÍA AVANZA. Y LOS DELINCUENTES INFORMÁTICO TAMBIEN SE MODERNIZA EN SUS MODALIDADES.

10. ¿Qué acciones significativas y exitosas han realizado las entidades competentes para proteger el derecho al patrimonio en el delito de fraude informático?

- ORIENTACION A LA SOCIEDAD SOBRE LOS DELITOS INFORMATICOS.
- PATRULLAJE VIRNALES CONSTANTES EN EL INTERNET.

11. Hay quienes señalan que la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó deficiente ya que no contó con personal calificado, logística y recursos que le permitan llevar a cabo operativos de prevención e intervención en estos delitos en el periodo 2021 ¿cuál es su posición al respecto?

LAS NECESIDADES DE RECURSO DE PERSONA CALIFICADO Y LOGISTICO ES CONSTANTE, PERO LA FORTALEZA QUE TIENE LA DIVINDAT ES SU PERSONAL, GRACIAS ELLOS SE REALIZA LOS OPERATIVOS Y PREVENSION.

12. ¿Algo más que dese agregar / comentarios / sugerencias?

- FORTALECER LA UNIFICACION DE IDEAS ENTRE LA PNP y MP.
- PREPARACION CONSTANTE EN LOS DELITOS INFORMATICO.

SELLO del entrevistado	FIRMA del entrevistado
SP - 30528564 VICTOR ESPINOZA PRADO SOS. PNP	

GUÍA DE ENTREVISTA

Dirigido a expertos en ciberdelito / policías / fiscales

TÍTULO: El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce*. 2021
Entrevistado: Julio Ronald Larico Rodriguez
Cargo / grado académico S2 PNP.
Institución donde labora: Policia - Divindat.

OBJETIVO GENERAL

Determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia en el periodo 2021

1. ¿En qué consiste el fraude informático cometido a través del *E-commerce*?

* Consiste en la creación de plataformas virtuales de comercio electronico, las cuales son mostradas a potenciales victimas mediante publicidad engañosa, posicionamiento de búsqueda en Google, y tienen como finalidad obtener información confidencial, de tarjetas bancarias, contraseñas, claves token. entre otros, los cuales son utilizados para cometer el delito de Fraude Informatico.

2. ¿Cuál fue el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

- Se creo la fiscalia Especializada contra la Ciberdelincuencia, persiguiendo de manera especializada y conjunta el Delito Informatico
- Han realizado Charlas y capacitaciones para que puedan afrontar este delito.

3. ¿Qué recomendaciones haría para que el Ministerio Público de Lima centro mejore su desempeño en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

* Poner Enfasis en las solicitudes de información a los bancos, a fin que estos brinden la información de manera casi inmediata
* Tramitar y obtener resultados en las medidas limitativas del Levantamiento del secreto de las comunicaciones y Levantamiento del secreto bancario.

4. Hay quienes sostienen que el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce*, resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021 ¿cuál es su posición al respecto?

- Se debe a la falta de información proporcionada por las entidades, así también a que la ley no especifica el delito informatico ya que hay varios vacios legales que hacen que este delito en su mayoria quede impune.

.....

.....

.....

.....

.....

.....

.....

OBJETIVO ESPECÍFICO 1

Evaluar el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

5. ¿Cuál cree que fue el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

- Charlas preventivas.
- Coordinación constante con dp. PNP. para orientar a la ciudadanía y puedan evitar e identificar los delitos informáticos.

.....

.....

.....

.....

6. ¿De qué manera la Oficina Técnica del Ministerio Público podría mejorar su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

- falta una fluida comunicación con el personal PNP que investiga los delitos informáticos.

.....

.....

.....

.....

.....

.....

.....

7. Hay quienes señalan que el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó limitado ya que no contó con implementos tecnológicos y logística especializada que le permitió llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos en el periodo 2021 ¿cuál es su posición al respecto?

- Restructuración de la norma, falta de información por parte de las empresas.

.....

.....

.....

OBJETIVO ESPECÍFICO 2

Evaluar la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

8. ¿Cuál fue la labor que desarrolló la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

*- Charlas preventivas, conferencias, atención al público con la finalidad de hacerles conocer las modalidades del delito informático.

.....

.....

9. ¿Qué recomendaciones haría para que la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional mejore su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

- Una mejora en la adquisición de equipos tecnológicos.
- Software licenciados y actualizados

10. ¿Qué acciones significativas y exitosas han realizado las entidades competentes para proteger el derecho al patrimonio en el delito de fraude informático?

- Publicidad advirtiendoles a la ciudadanía que no brinden información personal, ni contraseñas.

11. Hay quienes señalan que la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó deficiente ya que no contó con personal calificado, logística y recursos que le permitan llevar a cabo operativos de prevención e intervención en estos delitos en el periodo 2021 ¿cuál es su posición al respecto?

- Que si, falta una mayor - incremento del personal, Tecnico, Logistico, asi tambien un cambio en las leyes.

12. ¿Algo más que dese agregar / comentarios / sugerencias?

por el momento, no.

SELLO del entrevistado	FIRMA del entrevistado
SA-31636976 Julio Ronald LARICO RODRIGUEZ S2 PNP	

GUÍA DE ENTREVISTA

Dirigido a expertos en ciberdelito / policías / fiscales

TÍTULO: El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce*. 2021
Entrevistado: JOSE MIGUEL MILLONES VELÁSQUEZ.....
Cargo / grado académico.....SUPERIOR COMPLETA
Institución donde labora:.....PNP.....

OBJETIVO GENERAL

Determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia en el periodo 2021

1. ¿En qué consiste el fraude informático cometido a través del *E-commerce*?

.....
-SON ACCIONES COMETIDAS A TRAVÉS DEL COMERCIO
ELECTRÓNICO, CARACTERIZADA POR LA VENTA HUY
CONCURRIDA DE LAS PERSONAS EN LA PLATAFORMA
DE INTERNET.
.....
.....
.....
.....
.....
.....
.....
.....

2. ¿Cuál fue el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

LA APARICIÓN Y EVOLUCIÓN DE LAS TECNOLOGÍAS Y HERRAMIENTAS INFORMÁTICAS EN LOS ÚLTIMOS AÑOS, SON DE GRAN AYUDA PARA LA HUMANIDAD, EL HOMBRE COMO SER EVOLUCIONA, SIENDO ESTE CASO UN CLARO EJEMPLO DE SU EVOLUCIÓN; SIN EMBARGO, ESTE DESARROLLO HA PERMITIDO QUE LA CRIMINALIDAD AVANCE, BURLANDO LAS MEDIDAS DE SEGURIDAD ADOPTADA POR LAS EMPRESAS QUE BRINDAN EL SERVICIO DE COMERCIO ELECTRÓNICO, CREANDO BASE DE DATOS FALSOS, COMETIENDO "DELITOS INFORMÁTICOS", POR LO TANTO, NACE LA PERSECUCIÓN DEL ESTADO REPRESENTADO POR EL MINISTERIO PÚBLICO.

3. ¿Qué recomendaciones haría para que el Ministerio Público de Lima centro mejore su desempeño en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

MEJORAR LOS CANALES DE CAPACITACIÓN A LOS OPERADORES DE JUSTICIA, EN ESPECIAL A LA PNP, Y A LOS FISCALES DE TURNO, COMO PRIMEROS RESPONDIENTES FRENTE A HECHOS DE CIBERDELINCUENCIA.

4. Hay quienes sostienen que el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce*, resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021 ¿cuál es su posición al respecto?

TOTALMENTE DE ACUERDO, LA FALTA DE TECNOLOGIAS HACE QUE LA DELINCUENCIA A TRAVES DE ESTOS MEDIOS SIGA GENERANDO DAÑOS A LA SOCIEDAD.

OBJETIVO ESPECÍFICO 1

Evaluar el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

5. ¿Cuál cree que fue el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

CREAR PUENTES QUE AYUDEN A MITIGAR LOS AVANCES DE LOS DELITOS COMETIDOS POR LOS MEDIOS ELECTRÓNICOS

6. ¿De qué manera la Oficina Técnica del Ministerio Público podría mejorar su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

FORTALECER LA CAPACITACION A LAS PERSONAS, A LA COLECTIVIDAD

.....

.....

.....

.....

.....

.....

.....

.....

.....

7. Hay quienes señalan que el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó limitado ya que no contó con implementos tecnológicos y logística especializada que le permitió llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos en el periodo 2021 ¿cuál es su posición al respecto?

EFECTIVAMENTE, SE DESCONOCE EL PROCEDIMIENTO, LA APLICACIÓN DE HERRAMIENTAS A SEGUIR, TENER EN CUENTA QUE ESTE TIPOS DE DELITOS SE PRODUCE DESDE UN ORDENADOR QUE MUCHAS VECES NO DOMICILIA EN EL PERÚ.

OBJETIVO ESPECÍFICO 2

Evaluar la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

8. ¿Cuál fue la labor que desarrolló la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

ESTÁN INICIANDO ESTE TIPO DE LABORES, YA QUE ES UN DELITO POCO PERSEGUIDO POR LA JUSTICIA.

9. ¿Qué recomendaciones haría para que la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional mejore su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

CAPACITAR AL PERSONAL POLICIAL DEDICADOS A LA PERSELUSIÓN DE ESTE TIPO DE DELITOS, A LA FECHA ESTA CAPACITACIÓN ES DÉBIL FALTA DE CAPACITADORES IDONEOS.

10. ¿Qué acciones significativas y exitosas han realizado las entidades competentes para proteger el derecho al patrimonio en el delito de fraude informático?

NO SE CONOCE A LA FECHA, SON POCOS LOS LOGROS CONOCIDOS POR LOS MEDIOS TELEVISIVOS.

11. Hay quienes señalan que la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó deficiente ya que no contó con personal calificado, logística y recursos que le permitan llevar a cabo operativos de prevención e intervención en estos delitos en el periodo 2021 ¿cuál es su posición al respecto?

TOTALMENTE DE ACUERDO, DEBERÍA SER LA UNIDAD POLICIAL QUE DEBA CONTAR CON LOS MEJORES EQUIPOS Y LOS MEJORES INVESTIGADORES EN EL PAÍS.

12. ¿Algo más que dese agregar / comentarios / sugerencias?

NO.

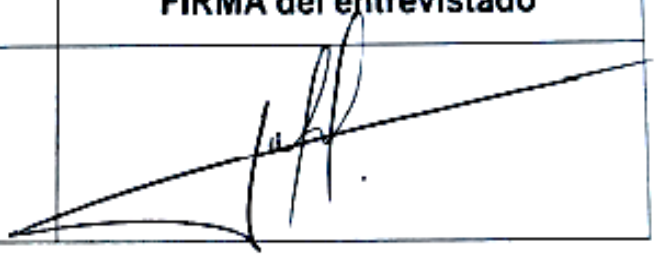
.....

.....

.....

.....

.....

SELLO del entrevistado	FIRMA del entrevistado
SA-31517654 J. MILLONES V. ST PNP.	

GUÍA DE ENTREVISTA

Dirigido a expertos en ciberdelito / policías / fiscales

TÍTULO: El rol del Ministerio Público de Lima centro en el delito de fraude informático cometido a través del *E-commerce*, 2021

Entrevistado: Rodriguez Flores, Diana.

Cargo / grado académico: SIPNP

Institución donde labora: DIVINDAT

OBJETIVO GENERAL

Determinar el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia en el periodo 2021

1. ¿En qué consiste el fraude informático cometido a través del *E-commerce*?

Es una operación que se realiza a través del internet mediante el cual se fijan operaciones (compras) que posiblemente nunca surjan, es decir, no se concretan.
Esta modalidad podría, mal llamarse fraude informatico, pues se trata de una estafa.
Vale decir, que si el autor, fabrica una página con el fin de realizar e-comerce, este se configuraría Delito Informatico. - J.I.

2. ¿Cuál fue el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

- Persiguir los Delitos contra el patrimonio - Estafa Agravada Art. 196-A N°5.

- Pedir información a los bancos, centros comerciales (Datos consignados), sea virtual o física.

3. ¿Qué recomendaciones haría para que el Ministerio Público de Lima centro mejore su desempeño en la persecución del delito de fraude informático cometido a través del *E-commerce* en la lucha contra la ciberdelincuencia?

→ Actuar de manera urgente e inaplazable en las diligencias preliminares.

4. Hay quienes sostienen que el rol del Ministerio Público de Lima centro en la persecución del delito de fraude informático cometido a través del *E-commerce*, resultó poco significativo ya que no contó con la infraestructura, logística y personal idóneo que le permita luchar contra la ciberdelincuencia en el periodo 2021 ¿cuál es su posición al respecto?

Que aún se encuentra en implementación.

OBJETIVO ESPECÍFICO 1

Evaluar el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

5. ¿Cuál cree que fue el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

La elaboración de analisis y pericias a los equipos tecnologicos vinculados a un Delito Informatico.

6. ¿De qué manera la Oficina Técnica del Ministerio Público podría mejorar su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

→ La implementación de equipos es primordial.

7. Hay quienes señalan que el rol de la Oficina Técnica del Ministerio Público en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó limitado ya que no contó con implementos tecnológicos y logística especializada que le permitió llevar a cabo una correcta y adecuada investigación con la finalidad de identificar a los ciberdelincuentes que cometen estos ilícitos en el periodo 2021 ¿cuál es su posición al respecto?

→ Siempre habrán comentarios, pero el compromiso y el abastecimiento de equipos es necesario para una optima resolución de investigaciones.

OBJETIVO ESPECÍFICO 2

Evaluar la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático en el periodo 2021

8. ¿Cuál fue la labor que desarrolló la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

→ Investigar el delito cometido.

9. ¿Qué recomendaciones haría para que la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional, mejore su desempeño en la salvaguarda del derecho al patrimonio en el delito de fraude informático?

→ Equipos tecnologicos.

10. ¿Qué acciones significativas y exitosas han realizado las entidades competentes para proteger el derecho al patrimonio en el delito de fraude informático?

→ Publicidad preventiva.

11. Hay quienes señalan que la labor que desarrolla la División de Investigaciones de Delitos de Alta Tecnología de la Policía Nacional en la salvaguarda del derecho al patrimonio en el delito de fraude informático resultó deficiente ya que no contó con personal calificado, logística y recursos que le permitan llevar a cabo operativos de prevención e intervención en estos delitos en el periodo 2021 ¿cuál es su posición al respecto?

→ Que sí, se requiere mayor personal, logística, etc. que facilite el proceso de investigación.

12. ¿Algo más que dese agregar / comentarios / sugerencias?

Para la persecución de este delito es recomendable la constante capacitación de las personas que se encargan de las investigaciones.

SELLO del entrevistado	FIRMA del entrevistado
Andrea E. Rodríguez Flores S... PNP CIP: 31478012	