



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE DERECHO Y HUMANIDADES

ESCUELA PROFESIONAL DE DERECHO

Fraude informático y el derecho al patrimonio en Lima Norte 2023

**TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
Abogado**

AUTOR:

Loarte Poma, Antinogenes Liverato (orcid.org/0000-0002-4210-7282)

ASESOR:

Dr. Quiroz Rosas, Juan Humberto (orcid.org/0000-0003-1434-4376)

LÍNEA DE INVESTIGACIÓN:

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

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Fortalecimiento de la democracia liderazgo y ciudadanía

LIMA - PERÚ

2023

Dedicatoria

Dedico a mis padres, hermanos y hermanas, y a mis sobrinos menores quienes me dieron apoyo y aliento día a día para concluir con mi objetivo.

Agradecimiento

Agradecimiento: A mi asesor, el Dr. Quiroz Rosas Juan Humberto y a mis profesores de la UCV de la Escuela Profesional de Derecho, ya que ellos me motivaron a continuar y concluir con la actual tesis.



UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO**

Declaratoria de Autenticidad del Asesor

Yo, QUIROZ ROSAS JUAN HUMBERTO, docente de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Fraude Informático y El Derecho al Patrimonio en Lima Norte 2023", cuyo autor es LOARTE POMA ANTINOGENES LIVERATO, constato que la investigación tiene un índice de similitud de 11.00%, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

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

LIMA, 01 de Diciembre del 2023

Apellidos y Nombres del Asesor:	Firma
JUAN HUMBERTO QUIROZ ROSAS DNI: 09458935 ORCID: 0000-0003-1434-4376	Firmado electrónicamente por: JHQUIROZR el 01- 12-2023 11:05:24

Código documento Trilce: TRI - 0675643



**FACULTAD DE DERECHO Y HUMANIDADES
ESCUELA PROFESIONAL DE DERECHO**

Declaratoria de Originalidad del Autor

Yo, LOARTE POMA ANTINOGENES LIVERATO estudiante de la FACULTAD DE DERECHO Y HUMANIDADES de la escuela profesional de DERECHO de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, declaro bajo juramento que todos los datos e información que acompañan la Tesis titulada: "Fraude Informático y El Derecho al Patrimonio en Lima Norte 2023", es de mi autoría, por lo tanto, declaro que la Tesis:

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

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

Nombres y Apellidos	Firma
LOARTE POMA ANTINOGENES LIVERATO DNI: 10403184 ORCID: 0000-0002-4210-7282	Firmado electrónicamente por: ALOARTEPO18 el 18- 12-2023 23:33:36

Código documento Trilce: INV - 1531604

Índice de contenidos

CARÁTULA	I
DEDICATORIA	II
AGRADECIMIENTO	III
DECLARACIÓN DE AUTENTICIDAD DEL ASESOR	IV
DECLARACIÓN DE ORIGINALIDAD DEL AUTOR	V
ÍNDICE DE CONTENIDOS	VI
ÍNDICE DE TABLAS	VII
RESUMEN	VIII
ABSTRACT	IX
I. INTRODUCCIÓN	1
II. MARCO TEÓRICO	4
III. METODOLOGÍA	11
3.1 Tipo y Diseño de Investigación	11
3.2 Categorías, subcategorías y matriz de categorización.....	11
3.3 Escenario de estudio	12
3.4 Participantes	13
3.5 Técnicas e instrumentos de recolección de datos	15
3.6 Procedimientos	16
3.7 Rigor Científico	19
3.8 Método de Análisis de información	20
3.9 Aspectos éticos	21
IV. RESULTADOS Y DISCUSIÓN.....	23
V. CONCLUSIONES	38
VI. RECOMENDACIONES	39
REFERENCIAS	40
ANEXOS	46

Índice de tablas:

Tabla 1 : Lista de participantes.....	13
Tabla 2 : Trayectoria metodológica de la investigación.....	19
Tabla 3 : Validación de Instrumento de la Guía de Entrevista	20
Tabla 4 : Lista de documentos.....	23
Tabla 5 : Respuesta de los entrevistado según las categorías	26
Tabla 6 : Resumen de coincidencias y discrepancias entre los entrevistados....	36

Resumen

El presente trabajo de investigación titulado “Fraude Informático y el derecho al Patrimonio en Lima Norte 2023” tuvo como objetivo general: Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023.

Referente al marco metodológico nuestra investigación es de enfoque cualitativo, de tipo básico, diseño de teoría fundamentada y nivel descriptivo. Los métodos de análisis de datos utilizados son analítico, inductivo, interpretativo, descriptivo y comparativo. Como también, la técnica que se empleó para la recolección de datos fue la entrevista, los instrumentos aplicados fue la guía de la entrevista a 8 expertos en fraude informático.

Se recopiló informaciones a través de plataformas virtuales indexadas y científicas. Con el desarrollo y avance de las Tics germina un nuevo fenómeno criminal relacionado al uso de ordenadores y de buscadores virtuales, sistemas telemáticos y su almacenamiento y procesamiento de información, acceden a las combinaciones de las cuentas comerciales, financieras, bancarias y/o individuales. En Latinoamericanos se está implementando diversas medidas. En nuestro país se aprobó el convenio sobre la ciberdelincuencia mediante la Resolución Legislativa N° 30913, 12 de febrero 2019, ratificado por el Ejecutivo con Decreto Supremo N° 010-2019-RE el 10 de marzo 2019.

Palabras clave: Fraude informático, derecho al patrimonio, obtención de datos ilegales, pérdidas materiales, daños morales.

Abstract

The general objective of this research work entitled “Computer Fraud and the Right to Property in Lima Norte 2023” was: Determine the way in which the crime of computer fraud violates the right to property in Lima Norte 2023.

Regarding the methodological framework of our research, it has a qualitative approach, basic type, grounded theory design and descriptive level. The data analysis methods used are analytical, inductive, interpretive, descriptive and comparative. Also, the technique used to collect data was the interview, the instruments applied were the interview guide for 8 experts in computer fraud.

Information was collected through indexed and scientific virtual platforms. With the development and advancement of ICTs, a new criminal phenomenon arises related to the use of computers and virtual search engines, telematics systems and their storage and processing of information, access to combinations of commercial, financial, banking and/or individual accounts. Various measures are being implemented in Latin America. In our country, the agreement on cybercrime was approved through Legislative Resolution No. 30913, February 12, 2019, ratified by the Executive with Supreme Decree No. 010-2019-RE on March 10, 2019.

Keywords: Computer fraud, right to property, obtaining illegal data, material losses, moral damages.

I. INTRODUCCIÓN

El desarrollo de la tecnología propicia el auge de las comunicaciones, a través de ello se abre la puerta para el inicio y desarrollo de contravenciones, manipulando medios informáticos con la entrada, cambio, avería o destrucción de archivos y datos informáticos lo realizan de cualquier lugar de donde está conectado al internet.

A partir de las últimas etapas del siglo XX, emprendió el auge de la ciencias aplicadas de la automatización e informaciones, el hardware fue más pequeño y versátiles y el software más instantáneo y amigable al usuario, con la invención de los teléfonos móviles integrados con internet y la conexión a otros dispositivos, integrados los ordenadores de las instituciones bancarias, empresas privadas, e instituciones de servicios, así como la venta por cantidades de los ordenadores y con uso frecuente de las mismas; esto hace posible el incremento de los delitos informáticos y uno de ellos es el fraude informático.

A consecuencia del aumento del fraude informático, los países impulsan diversas medidas para proteger los archivos de los usuarios que se hallan asignados en el internet. Como también, la modernización provocó un aumento del teletrabajo y el comercio electrónico. Lo cual motivó la propagación de los engaños en las redes digitales; contravenciones que violan las normas establecidas de protección al usuario. Las naciones del mundo tienen una gran responsabilidad en la regulación de la política de seguridad contra el delito informático y la reglamentación sobre la inteligencia artificial (Bokovnya,2020).

En el ámbito internacional, mediante la observación jurídico comparativo de los delitos informáticos latinoamericanos, realizado en estos últimos años, la vulneración de datos personales en los países integrantes, cuando se trata del delito de robo de identidad digital, tiene promulgado legislaciones pertinentes: Los países como República Dominicana, Puerto Rico y Costa Rica. De los cuales, por ejemplo, los ciudadanos de Costa Rica tienen como derecho esencial el amparo de las identificaciones propias, cada ciudadano tiene control de sus datos personales y la información y manejo de las mismas de manera constitucional, vale decir que la carta magna de ese país la ampara como un derecho esencial al resguardo de los datos, fichas y archivos privados informáticos (Rivera,2019).

Por otro lado, en el Perú los ciberdelitos amenazan al aspecto económico, a un sistema de vida democrática, las autonomías y los bienes y servicios. La cantidad de archivos hurtados en 2022 es de 8500 millones de registros de datos personales que se comercializan y utilizan, los cuales fueron ocasionados por los ataques de maniobra en Internet. El cibercriminal continúa evolucionando al ritmo del contexto social, económico y tecnológico (Ospina, 2020).

En año 2021, en el Perú se registró 5,620 acusaciones, en año 2022 se inspeccionó 3,946 acusaciones por delitos informáticos ante la Dirección de Investigación Criminal de Alta Tecnología (DIVIDANT) que corresponde a la Policía Nacional del Perú. De los cuales 135 y 229 facinerosos fueron detenidos. Las detenciones representan solo un 2, 4% para el año 2021 en relación a un 5.8% en el año 2022 siendo un índice muy bajo de detención de las personas que cometen delitos informáticos. Es una información publicada en diario oficial (El Peruano, 17 septiembre 2023).

Si no se investiga este problema, los resultados se pronostican terriblemente negativas; con la utilización de la estafa por internet, se incrementa los delitos cibernéticos, esto se debe al uso frecuente de los medios digitales, si incluimos en la Ley de delitos informáticos la modalidad de delito informático “Phishing, Vishing, Smishing, Carding y Pharming” mediante esta modalidad la interacción del sujeto pasivo con el activo es mínimo, puesto que la obtención de los datos bancarios de los afectados son imperceptibles, porque se utilizan desvió de páginas, luego hacen uso ilegal, por lo que no hay engaño, como la que requiere nuestro Código Penal (Fuente, 2021).

Nuestro supuesto de la investigación fue, que, si no se incluye los delitos phishing, vishing, smishing, carding y pharming en nuestro Código Penal y, además, no se incrementa medidas y métodos de control y protección para combatir cualquier tipo de delito informático, la cibercriminalidad continuará amenazando y dañando el patrimonio de las personas y de la nación.

Por lo explicado, nuestro enfoque de investigación es cualitativa y tiene una relevancia científica, por lo que es una técnica de actuación concreta de recojo de información particular, como la utilización de la técnica de entrevista y del instrumento

guía de la entrevista , donde recogemos información particular de hechos o materia de la investigación, mediante la cual describiremos principales hechos delictivos y las consecuencias desde el punto vista jurídico, como pérdida del patrimonio mediante el engaño, robo y fraude utilizando el internet (Sánchez, 2021).

Enunciamos el subsiguiente problema general de investigación: ¿De qué manera el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023? Tenemos como problemas específicos: ¿De qué manera se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023?, ¿Cuáles son los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023?

El presente trabajo tenemos como justificación teórica de la investigación, como sabemos que en esta pandemia del COVID 19, se incrementaron trabajos remotos y las sistematizaciones crediticias analógicos, que facilitaron el incremento de los ataques a los archivos propios de los consumidores de la banca por internet, mediante engaños para hurtar y sustraer sus dineros depositados, como también, según los datos estadísticos de la PNP, de los años 2020 y 2021 según ONPC Observatorio Nacional de Política Criminales se incrementaron las denuncias de ciberdelitos, en el que pasamos de 25% a 65% más denuncias por esta forma de infracción (Chero, 2022). A sí mismo, la justificación práctica incurre en que este trabajo de investigación puede ser útil para dar luces para la mejora en el campo del sistema jurídico informático. Como también, la justificación metodológica incurre en la información y el procesamiento de información de jurisprudencias, caracteres legales y la entrevista a autores, tratadistas y concedores sobre este asunto tratado, utilizando el método científico.

Es por esta razón, planteamos como objetivo general: Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023, como objetivos específicos: Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023, Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023.

II. MARCO TEÓRICO

El fraude informático y la vulneración del derecho al patrimonio, fue considerado novedoso y muy actualizado en las búsquedas a través de plataformas virtuales con material científico y de diversas fuentes como Cybertesis, EBSCO, repositorio de la UCV y archivos SCIELO, entre otros. Por otra parte, se masifican celulares, tablet, laptop, PC, entre otros, todas conectadas a la red de internet. Con estos avances tecnológicos, surgen fenómenos criminales relacionado con el delito informático.

Los antecedentes de la presente investigación correspondieron el análisis de revistas, informes científicos y libros, a través de plataformas virtuales indexadas tesis a nivel nacional e internacional.

En cuanto a los antecedentes internacionales, en Colombia, una tesis de maestría sustentada por Peña (2023) sobre delitos cibernéticos, menciona que cada vez muchas personas utilizan internet y por lo tanto se incrementan los ataques cibernéticos a instituciones financieras, bancarias, comerciales, afectando a la población y siendo una carga a resolver para el estado.

Además, en México, una tesis sustentada por Vences (2019) sobre penalización de los delitos informáticos, en la cual afirma que el derecho informático, aparece como una nueva rama del derecho, ya que el auge de la información por medios de aparatos y equipos interconectados a internet, requieren nuevos procedimientos reglamentarios, garantizando la protección de los datos que almacena en su memoria.

Referente a los antecedentes nacionales, en Perú, Tuesta (2022) en su tesis presentado para obtener el título de abogado, postula que el fraude informático es uno de los delitos que se han incrementado en los últimos años afectando los derechos primordiales de las personas en Lima, esto se incrementa por la dificultad de la identificación.

Como también, Chávez (2018) en su tesis para optar el grado de Doctor en derecho, menciona que los delitos cometidos contra los secretos de claves en el régimen digital afectan a los derechos fundamentales de las personas.

Igualmente, el Perú, Goñi (2021) en su tesis, para obtener el título de abogado, menciona que, con el uso frecuente del Internet surge una nueva era del crimen informático.

Asimismo, en la Universidad Nacional Federico Villareal, mediante la tesis de Blossiers (2018), donde indica que no existe un conveniente procedimiento legal sobre delitos informáticos, vale decir lo que no es suficiente para el amparo de los derechos de los individuos, compañías e instituciones.

De la misma manera, Rivera (2022) en su tesis para optar el grado de doctor en derecho, menciona que los delitos informáticos realizados, especialmente por los funcionarios, afectan a las instituciones privadas como públicas en forma negativa.

De otro lado, para Ancco (2021) en su tesis para obtener título de abogado sostiene que, el crimen organizado tiene una relación positiva respecto a su cometido delictiva, sugiriendo que el Poder Judicial incremente la capacitación a los operadores.

Con el fin de profundizar sobre la categoría concerniente al fraude informático, Mayer y Olivera (2020), expone en su artículo indexada de la revista chilena. Que el nombre de delito informático se refiere a una operación que recopila las características definitorias del concepto de delito, que son la explotación de elementos informáticos, mediante la vulneración los derechos de los titulares de los quipos Informáticos, dispositivos físicos o los mecanismos lógicos. Por otro lado, sostiene el peruano, Espinoza (2022), que los informes referentes a las estafas cibernéticas ejecutadas por medios digitales utilizando el internet, mediante diversas modalidades, ocasiona un peligro latente para la población, una dificultad para la policía, por la complejidad y la especialización de robo por internet y un reto más para el gobierno nacional. Muchos casos no son denunciados, ni reportados; lo cual, ocasiona dificultad en la identificación de los sujetos autores del delito informático, para la PNP y los fiscales.

Referente al fraude informático en el Artículo 8 de la Ley 30096 establece que, a través de la TIC, si para su propio provecho o de otra persona de modo ilegal, utilizando el diseño, ingreso, modificación, eliminación, interrupción, duplicación de fichas informáticos, se castiga con encarcelamiento no menor de 3, ni mayor de 8 años y con 70 a 120 días multa. En el mismo artículo tenemos un agravante de un encierro en la prisión no menor de 5 ni mayor de 10 años y de 80 a 140 días multa, cuando quebranta, altera propiedades del estado reservados a sostenimiento de ayudas a los más necesitados. A sí mismo, en el convenio sobre la ciberdelincuencia (Que entró en vigor, el diciembre del 2019) en el artículo 8, dice; que los gobiernos suscritos deben

fomentar iniciativas legislativas, que impliquen prevenir, intervenir y sancionar a los que cometen delitos por internet, cometen estos hechos personas que trabajan en diferentes países.

Por otro lado, para el caso de la categoría **fraude informático**; según Jiménez (2017). Es una forma ilegal de beneficio propio mediante la alteración, destrucción, supresión o pérdida de datos o archivos almacenados en la memoria de equipos informáticos personales. Como también, Vinelli (2021). Manifiesta que en los años 2020 y 2021 se incrementaron operaciones comerciales virtuales, mediante el uso de las transacciones, con pagos y compras digitales que ha aportado varios progresos; como también ha ocasionado cuantiosas dificultades, uno de esas dificultades son el incremento de la actividad delictiva por medio de las redes del internet como el fraude informático. Para Arias (2021); en el fenómeno informático destaca los aspectos criminológicos: El primer aspecto es el riesgo, que gira en torno al "conocimiento". que los nuevos sistemas informáticos mejoren, se desarrollen con ordenadores que acumulan numerosa información, el mayor parte contenido versátil. En segundo lugar, el peligro aparece cuando se usa mal la información que se vuelve peligrosa en una sociedad ampliamente competitiva. La tecnología de la información multiplica el poder de quienes usan la información, pero al mismo tiempo crean y enfatizan desigualdad y cuestiona derechos y garantías de las personas que deben existir en un estado social y democrático. En tercer lugar, el abuso informático suele causar un gran daño a la víctima.

El Convenio de Budapest es actualmente el único instrumento internacional relacionado específicamente con delitos cibernéticos y que da respuesta a los delitos informáticos y de Internet; mediante el combate y persecución a los ciberdelincuentes, compartiendo los contenidos de las leyes relacionados a la ciberdelincuencia entre países, mediante la regulación del Ciberespacio. El primer convenio mundial referente la Ciberdelincuencia fue en Budapest el 23 de noviembre del 2001. Ingreso a vigencia internacional el 1 de julio del 2004 en Europa. En el Perú se dio la Resolución Legislativa N° 30913, el 12 de febrero 2019, ratificado por el Ejecutivo con Decreto Supremo N° 010-2019-RE el 10 de marzo 2019.

Referente a la categoría **derecho al patrimonio**, se entiende por la vulneración de un derecho, a las contravenciones de los derechos resguardados por la carta magna. Mediante esta contravención, llamado delito informático, se afecta el derecho al patrimonio, como son las propiedades de las personas; ya sea en dinero en efectivo, mercaderías, equipos electrónicos, alimentos, muebles e inmuebles, entre otras. Huamán (2020). Como también, referente a la categoría víctima del patrimonio, según Arias (2017). Afirma que, la categoría víctima del patrimonio, es concebir por víctima a al individuo que es dañada y afectada por la conducta del delincuente o criminal. Por su parte, García (2019), refiere que el bien jurídico protegido es la propiedad y la intimidad humana; sin embargo, muchos autores afirman que el delito informático afecta a muchos bienes protegidos y aun por proteger en el futuro ya que aparecerán nuevas formas de delincuencia. A sí mismo, Morena del Rio (2020) sostiene que existe una gran importancia de los bienes jurídicos tutelados en el espacio de las ordenanzas de carácter administrativa mediante atribuciones protectoras a los intereses de los propietarios.

Por otra parte, el **daño moral** es la frustración de las ventajas económicas esperadas, el detrimento del capital y las depresiones psicológicas por pérdida económica. Es algo no económico, que afecta el sentimiento de la persona. Al respecto Collque (2017) comenta que se manifiesta mediante la variación del momento moral como depresión, angustia, furia, miedo, furor, violencia, angustia, pavor, emociones de desaliento, desequilibrio, vacilación, pérdida del amor propio, ansiedad, sentimientos de desenlace o compensación, entre muchos sentimientos encontrados.

Relativo al marco jurídico, en la Carta Magna del Perú, en el Artículo 2, inciso 6 reconoce que todos tenemos derecho al servicio por computadoras, sean públicas o privadas, no proporcionen información que perturben la privacidad propia y de la familia. Si bien es cierto que nuestra Carta Magna reconoce el uso de la informática y otros medios, así como también prohíbe que se introduzca datos que afectan a las personas; sin embargo, no está configurado, el derecho a la protección contra el fraude informático que afecta a la propiedad de los consumidores de la malla de internet; por lo tanto, existe un vacío legal frente fraude informático al patrimonio. Así también, la Ley de Delitos Informáticos, Ley N° 30096, en el Art. 8 tipifica al fraude informático

como un delito que tiene una pena privativa de libertad con, no menor de 3 a 8 años, tiene su agravante cuando afecta el patrimonio de las instituciones públicas destinados a casos sociales, como albergues de ancianos, casas para discapacitados, orfanatos de niños abandonados, comedores populares, etc. con pena privativa de libertad no menor de 5 ni mayor de 10 años. Asimismo, en el Código Penal Peruano en el Artículo 245 Ocultamiento, omisión o falsedad de información. Generalmente lo hacen los administradores de bancos, financieras, de instituciones públicas y/o privadas, utilizando los medios virtuales. Serán reprimidos con encarcelamiento de 4 a 8 años. Como también, en nuestro Código Procesal Penal el Artículo 230, la Intrusión, grabación de conversaciones por teléfonos o de otras formas de comunicación y localización geográfica de las telefonías inalámbricas. Incluye la localización de datos de archivos informáticos privados o públicos por medio de la intervención del fiscal. Referente a levantamiento de documentos, de datos y/o archivos informáticos. Artículos, 231, 232, 233 y 234.

Por otro lado, habiendo revisado teoría de base científica, los expertos Peña & Almanza (2010) en su libro teoría del delito, sostiene que el funcionalismo moderado propuesta por el abogado y jurista alemán Claus Roxin da razón que los recapitulaciones sobre el delito presentados por el finalismo (tipicidad, antijuridicidad, culpabilidad), pero con una orientación político-criminal, puesto que los presupuestos de la punibilidad deben estar orientados por los fines del Derecho penal, por lo que estas categorías jurídicas no son sino instrumentos de una valoración político-criminal y derecho criminal. Si un estado no tiene política criminal que armonice una prevención del delito, mediante la administración de justicia y tenga objetivo de readaptación en la sociedad de manera general, estaría condenado a la frustración, fracaso en la lucha contra la delincuencia.

Por otra parte, el tratadista salvadoreño, Arias (2021), plantea la teoría del delito aplicado al ciberdelito, que la teoría del delito proporciona materiales teóricos que permite constituir que un suceso ejecutado por el sujeto es necesariamente ese mismo suceso. Igualmente, el tratadista peruano Espinoza (2022) en su libro Delitos Informáticos y nuevas modalidades delictivas en cuanto al fraude informático, **bien jurídico protegido o tutelado** es el **patrimonio**, son datos numéricos de monedas

que se transforman en dinero físico. **Tipicidad Objetiva**, es un **delito doloso**. En cuanto a **la conducta** es el esbozo, incorporación, variación, eliminación, suspensión, duplicación de archivos digitalizados o la administración ilegal de las mismas, ocasionado daño a terceros. **Sujeto activo**, cualquier persona con conocimientos informáticos, trabajadores de entidades financieras y/o bancaria, así como los operadores telefónicos. **Sujeto Pasivo**, cualquier persona, especialmente el que tenga poco manejo informático. **Tipicidad subjetiva**, es el **dolo**, con intención de apropiarse de un bien o hacer daño a otra persona.

Tenemos tipos de fraudes informáticos como: **fraude por internet**, los delincuentes utilizan la red de internet para interceptar las señales e ingresar a los datos privados y hacen transacciones lo hacen de cualquier lugar, **fraude por identidad**, sucede que se apropian de los detalles personales nombre, fecha de nacimiento, del domicilio actual o de los anteriores, teléfonos, numero de celular, contactos personales. **ciber extorción** mediante el empleo de identificaciones personales, fotos de familiares, y actividad económica de la víctima, como coacción, amenaza y chantaje solicitan dinero. Como también, los **ataques de virus o malware**, como a) **Adware** programas que brindan divulgación embaucadora, anuncios con contenido de representaciones pictóricas y audios, se reproducen automáticamente y luego le cobran por el servicio y/o entorpecen la continuidad de la actividad del usuario. **spyware** recopila de forma engañosa la información de la navegación del usuario, identificaciones propios y financieros, como los **keyloggers** utilizan la actividad del teclado para enviar información al ciberdelincuente, **gusanos** se responden en computadoras, originan errores en la malla, ocasionando consumo anormal de ancho de banda. d) **Troyano** ingresa escondidas en programas piratas, office, antivirus, se instalan envían información al ciberdelincuente, **ransomware** asume una intervención completa bloqueando o limitando la información del dueño del equipo, luego pide dinero a intercambio del desbloqueo o descifrar los ficheros del dispositivo, **botnets** son mallas de aparatos enquistados, contaminados que los delincuente informáticos emplean para atacar con despacho intensivo de correspondencia spam, **apps maliciosas**, una app desconocido en un dispositivo móvil solicita permisos, lo cual contamina nuestro aparato móvil y toma control de

credenciales, imágenes, videos, audios, etc.

Según la división de Investigación de Alta Tecnología- DIVINDAT- de la PNP o el Ministerio Público, las modalidades de Fraude Informático más comunes son:

Clonación de tarjetas de crédito: Modalidad delictuosa utilizando equipos electrónicos de averiguación de franjas magnéticas (skimmer) extraen los datos de la tarjeta de crédito, para copiar a una computadora y los pegan en otra tarjeta con los mismos datos de la tarjeta original, solicitan créditos en efectivos o hacen compras en los mercados, por internet.

phishing: se hace por medio de envíos de correos electrónicos engañosos para atraer a las personas hacia sitios web aparentes, de modo que instauren en ellos información personal; número de tarjetas de crédito, contraseñas, información de cuentas, dirección, con ello delinquen, **vishing**. Combina información obtenida mediante Phishing en SMS simulando una entidad bancaria con llamada telefónica engañosa para que la víctima brinde su token digital o clave SMS para una transacción financiera fraudulenta.

smishing: Mediante mensajes de textos en telefonía celular o de WhatsApp de un supuesto banco, alerta sobre una sospechosa compra con su tarjeta de crédito; alentándole a cancelar dicha compra, llamando a una banca falsa que le responde, en la cual le piden sus datos confidenciales, clave, etc.

carding: Compra por internet manipulando la información de tarjetas de crédito o débito, utilizan datos de 16 dígitos, fecha de vencimiento o código de verificación, **skimming** lee, examina rápidamente los códigos de tarjetas mediante **skimmer** (lectora de códigos).

pharming: utiliza software malicioso para redirigir a los usuarios descuidados hacia lugares falsificadas de sitios web, con finalidad de obtener datos personales.

keylogging: se introduce programa que lee todo lo que escribe y así obtener información de sus cuentas y datos personales, para cometer el fraude informático.

sniffing: Cuando el usuario se de la red pública wi-fi no protegida o no cifrada de esta maneta los hackers, obtienen datos de clientes de una entidad financiera o bancaria.

III. METODOLOGÍA

3.1. Tipo y diseño de investigación:

Tipo de investigación: empleada es **básica**. Este tipo de investigación teniendo como base a la **intención de la indagación**, es la investigación Básica, llamada también indagación pura, teórica o dogmática. Esta indagación se inicia con un marco teórico que persiste hasta el final de trabajo. El punto central es de extender las sapiencias científicas, sin contrastar con un aspecto pragmático o práctico (Muntané, 2010).

Diseño de investigación: Nuestro diseño de investigación fue fenomenológico, porque se basa en las experiencias individuales, particulares del de la persona experta o conocedor de un fenómeno, materia a investigar o hecho ocurrido. El diseño de indagación fenomenológico centra su atención en el ambiente natural de los sucesos ocurridos e experimentados o vivenciados por el entendido, que más profunda de lo cuantificable o numérico (Fuster, 2019) por esta razón, para investigar mediante el diseño fenomenológico, en nuestro caso investigado hemos utilizado la entrevista, mediante una guía de entrevista estructurada.

El enfoque de nuestra investigación fue cualitativo asumimos un contexto intrínseco y formado por inmensidad de situaciones o hechos. Con el enfoque cualitativo hemos privilegiado el análisis profundo y reflexivo de los significados específicos que forman parte de la realidad estudiada (Sánchez, 2019).

3.2. Categorías, subcategorías y matriz de categorización

Categoría 1: Fraude informático. Es una forma ilegal de beneficio propio mediante la alteración, destrucción, supresión o pérdida de datos o archivos almacenados en la memoria de equipos informáticos (Jiménez, 2017).

Las subcategorías son: Obtención de datos ilegales, sabemos que, mediante el fraude informático, se obtiene datos en forma clandestina, prohibida, oculta y solapada; con la intención de apoderarse de los patrimonios de las personas naturales y/o jurídicas, de ese modo son perjudicados en sus

diversas posesiones, las propiedades que mayoritariamente son afectadas mediante el delito de fraude informático son las pertenencias monetarias, seguido por robo de mercaderías utilizando la clonación de tarjetas de crédito. Así como también, la subcategoría eliminación de datos es cuando el delincuente borra las identificaciones, con la finalidad de perjudicar al usuario del banco, de la financiera y cualquier otra empresa.

Categoría 2: Derecho al Patrimonio. La categoría derecha al patrimonio se refiere a que toda persona por ley le corresponde proteger su privacidad económica, su propiedad, su finca, su interés, ahorros, etc.

Subcategoría **Pérdidas Materiales** se refiere al despojo de sus bienes económicos, muebles e inmuebles, mercaderías y/o de dinero generalmente representado en cifras de moneda, que los delincuentes cibernéticos las destinan a otros bancos y las retiran, dejando generalmente vacío las arcas de las personas agraviadas.

La subcategoría **Daños morales.** Es la pérdida no económica. De tipo psicológico; nos referimos a la angustia, pena, dolor causado por la pérdida de bienes muebles e inmuebles, mercaderías y/o del dinero. Se manifiesta en desespero, bajo de autoestima y la impotencia psicosocial por encontrarse truncado sus proyectos y metas; a causa del desfalco por los delincuentes que se esconde en las redes del internet.

3.3. Escenario de estudio: Para nuestra investigación, hemos entrevistado a los participantes en su zona de labores como: Instituciones Judiciales, fiscalías, Universidades, oficinas jurídicas privadas y comisarías, todos ellos localizados en Zona Lima Norte, encontramos a nuestra disposición profesionales expertos como; Fiscales en delitos informáticos, abogados penalistas particulares, policías especializados en delito informático y docentes universitarios con especialidad en derecho penal.

Igualmente, Los distritos geográficos que comprenden Lima Norte son: Los Olivos, San Martín, Comas, Caraballo, Puente Piedra, Santa Rosa y Ancón, como también Ventanilla y el Centro Poblado de Pachacútec. que en cuanto a

la demarcación judicial pertenece a Distrito Judicial Ventanilla - Lima Noreste.

3.4. Participantes: Los entrevistados en la investigación son preferiblemente entendidos sobre temas relacionados a delitos informáticos. Hemos entrevistado a 8 conocedores de la materia en delitos informáticos, como: abogados especializados en derecho penal (2), catedráticos universitarios en derecho penal (2), y policías expertos en delitos informáticos (2), fiscales (2). A continuación, detallamos mediante la tabla de la lista de participantes.

Tabla1. Lista de participantes.

Ítem	Nombres y apellidos	Profesión/Grado académico	Cargo/ Función	institución	Años de experiencia
1	Alejandro Beder Augusto Saldaña	Superior Expertos en Delitos Informáticos.	Sub Oficial Superior PNP	Comisaria de Independencia	30 años
2	Genry Mas Guivin	Superior -Técnico Expertos en Delitos Informáticos.	Sub Oficial Segunda- PNP	Santa Luzmila – Comas	15 años
3	Dr. Alejandro Asca Robles	Abogado- Especialidad Derecho penal	Independiente	Oficina-Puente Piedra- Lima Norte.	32 años
4	Mg. Poldark Saravia Gonzales.	Abogado- Especialidad Derecho penal	Catedrático en Derecho Penal	Universidad Cesar Vallejo	28 años
5	Dr. José Ismael Benites García.	Abogado- Especialidad Derecho penal	Catedrático en Derecho Penal	Universidad Cesar Vallejo	25 años
6	Mg. Violeta Jiménez Rufino	Abogado- Especialidad Derecho penal	Catedrático en Derecho Penal	Universidad Cesar Vallejo	14 años
7	Dr. Juan Carlos Martínez Castro,	Abogado-Penalista	Fiscal: Ministerio Público.	Ministerio Publico-	20 años
8	Dr. Raymond Fernando Vargas López	Abogado Penalista- Maestro en Derecho Penal, Procesal Penal y Gestión Pública	Asistente Fiscal –Lima Norte.	Ministerio Publico	12 años

Fuente propia 2023

Según la tabla de lista de participantes, observamos que el número de expertos son 8, de los cuales: los expertos 1 y 2 son policías conocedores de los delitos informáticos, expertos 3 y 4 abogados penalistas, expertos 5 y 6 son catedráticos en derecho penal y los expertos 7 y 8 son fiscales especializados en delitos informáticos, quienes trabajan junto con las policías de la división de investigación de alta tecnología y de crimen organizado (DIVINDANT), los cuales se encargan de prevenir, investigar y sancionar a los que cometen delitos cibernéticos y otros delitos conexos, junto con la Unidad Fiscal Especializada en Ciberdelincuencia de Lima y los jueces de penal de la jurisdicción correspondiente.

3.5. Técnicas e instrumentos de recolección de datos: Según Hernández (2017), **la técnica** que hemos utilizado en nuestra indagación es la **Entrevista**: “La entrevista es una técnica de recolección de datos mediante el llenado de un cuestionario con un informante experto en el tema” (p. 239). Por medio de la entrevista formal y estructurada obtendremos información experta para enriquecer nuestro trabajo de investigación, Así mismo, utilizando análisis de literaturas jurídicas y análisis documental.

La entrevista es uno de las técnicas empleadas en la investigación de las ciencias sociales, como el derecho es pertenece a las ciencias sociales; utiliza las técnicas e instrumentos de esta rama de la ciencia. En la entrevista el entrevistador prepara las preguntas con anticipación de acuerdo a temas que desea profundizar, entrevistando a los especialistas, expertos, probos, conocedores, peritos en la materia a investigar.

Esta técnica es muy eficiente y tiene una preponderancia de seguridad científica ya que, las preguntas debidamente validadas por los expertos de acuerdo a la materia a investigar y los objetivos son muy beneficios y seguras en los aportes para investigación.

La técnica de la entrevista tiene algunas características propias: A) Las preguntas que se hizo al entrevistado fueron flexibles, lo que permitió al investigador aumentar algún pensamiento sobre el tema que se está aclarando.

B) en la entrevista sostuvimos una conversación amena y amistosa siempre indagando, profundizando el tema de acuerdo a su percepción o experiencia del especialista. C) Hemos empezado con preguntas generales y abiertas, permitiendo que el especialista entrevistado extienda su opinión de forma autónoma sin generar controversias ni contradicción por el entrevistador, de las cuales hemos obtenido información que no están escritos en textos de consulta (Arias, 2021) por otra parte, hemos tenido la oportunidad de reafirmar nuestra información sobre el tema fraude informático y el derecho al patrimonio en Lima Norte 2023

Otra técnica empleada es la, técnica del **análisis documental**, según Dulzaides (2002). “El análisis documental es una forma de investigación técnica, un conjunto de operaciones intelectuales, que buscan describir y representar los documentos de forma unificada sistemática para facilitar su recuperación. Comprende el procesamiento analítico- sintético [...], incluye la descripción bibliográfica [...]”. Así como, la clasificación de las fuentes, anotación de datos o términos importantes para la investigación, observación y estudio de contenidos de gráficos, tablas y cuadros informativos referente al tema, como también internalizamos los resúmenes, comentarios de autores de textos y de especialistas en revistas indexadas.

Instrumentos de recolección de datos: En el **instrumento de recolección de datos** hemos utilizado la **guía de la entrevista** mediante un cuestionario estructurada, debidamente elaborada conforme a los objetivos generales y específica, como también, de acuerdo a las categorías y subcategorías, todas ella debidamente revisadas y validadas por expertos abogados con maestría en derecho penal y especializados en delitos informáticos. Preferiblemente hemos entrevistado a docentes universitarios en actividad en universidades nacionales o privadas, así como también hemos entrevistado a miembros de la policía nacional peritos expertos, especialistas en delitos informáticos. La guía de la entrevista está estructurada para poder profundizar nuestra indagación aprovechando la experiencia de los expertos en el tema a investigar en nuestro caso el Fraude Informático y el Derecho al

Patrimonio en Lima Norte 2023.

El instrumento del análisis documental es la **ficha de análisis documental**, mediante este trabajo intelectual el investigador extrae nociones importantes, trascendentes de la materia o campo de investigación, así como, personifica y proporcionar el acceso a los originales, de esta manera derivar del documento frases y lemas que correspondan de representación para cumplir con los objetivos y metas de la investigación. Por lo tanto, el instrumento del análisis documental es un procedimiento científico y metódico de investigación, mediante la recolección, clasificación, análisis e interpretación de datos referentes a un determinado contenido, conduce a la reconstrucción de conocimientos, al igual que otros instrumentos (Rizo, 2015).

3.6. Procedimientos: Para la investigación se realizó los siguientes pasos: 1ro. Referente a la labor de campo, en cuanto al procedimiento de la entrevista se coordinaron con los entrevistados y recurrimos a las oficinas privadas de los abogados que tienen la especialidad de derecho penal, 2do. A los altos jefes policiales se le entrevisto en sus comisarias, 3ro, En las aulas universitarias a los catedráticos que enseñan derecho penal, aprovechando el break de sus labores. 4to a los fiscales aprovechando su espacio en su labor de trabajo en el campo. Relativo a el fraude informático y derecho al patrimonio en Lima Norte 2023, los entrevistados brindaron sus servicios contestado las preguntas de la guía de entrevista, en forma amena y satisfacción, nos sugirieron varios puntos para con el desarrollo de investigación.

Profundizamos nuestras dudas mediante la entrevista estructurada, una entrevista debidamente elaborada conforme a los objetivos generales y específica, como también, de acuerdo a las categorías y subcategorías, todas ella debidamente revisadas y validadas por expertos abogados con maestría en derecho penal y preferiblemente que sean docentes universitarios en actividad, en universidades nacionales o privadas. Para realizar la entrevista nos apersonamos a los lugares indicados para hacer los conversatorios amigables y abiertas sobre el tema a tratar, utilizando el cuestionario ya elaborado y

posteriormente analizaremos los datos obtenidos de la entrevista y confeccionamos las conclusiones de nuestra entrevista son abiertas y de acuerdo a los objetivos y categorías y subcategorías de nuestro trabajo de Investigación.

En la entrevista el entrevistador fue muy amable, amigables cortes y sobre todo reputaba las respuestas a las dudas planteadas para que nos aclare sobre un asunto que domina el experto por su experiencia personal. Estuvieron muy entusiasta al contestar los cuestionarios abiertas los entrevistados, entrevista, los señores propietarios.

Participaron en la entrevista son 8 expertos de los cuales: los expertos 1 y 2 fueron policías concedores de los delitos informáticos, expertos 3 y 4 abogados penalistas, expertos 5 y 6 son catedráticos en derecho penal y los expertos 7 y 8 son fiscales especializados en delitos informáticos, quienes trabajan junto con las policías de la división de investigación de alta tecnología y de crimen organizado (DIVINDANT), los cuales se encargan de prevenir, investigar y sancionar junto con la fiscalía y los jueces de penal a los que cometen delitos cibernéticos y otros delitos conexos.

Los entrevistados quedaron muy complacidos y agradecidos y alentaron este tipo de investigación, manifestando que el tema que se trató es muy interesante, en vista que la comisión de delitos informáticos es muy frecuentes en la realidad actual de nuestra sociedad y que este tipo de delitos afectan al patrimonio de los usuarios, especialmente a los que tienen poco conocimiento del manejo de la informática y redes sociales; siendo los más afectados los usuarios que utilizan softwares gratuitos ya que son inseguras y los más vulnerables son los adultos mayores, especialmente que utilizan sus tarjetas de débito y crédito de manera muy confiada. Además, manifestaron que estos temas de delitos informáticos son nuevos en la indagación de los delitos que se ejecutan en nuestro país.

En esta indagación realizamos el análisis de las normas nacionales e internacionales referente al delito de fraude informático, las cuales dieron un aporte responsable para el desarrollo y posterior sustentación de la

investigación.

Se realizó el **análisis documental** desde la identificación de fuentes confiables utilizando el Excel para la revisión de literatura científica, donde se recopiló los siguientes datos, autor, título, lugar, objetivo general, enfoque diseño de investigación, muestra, instrumentos, método de análisis aplicado, resultado obtenido, conclusiones, resúmenes, dimensiones, definiciones, teorías y referencias incluido el link, de 50 autores, luego se prosiguió, con la siguiente secuencia:

Primero; con la exploración e identificación del problema, referente al fraude informático y el derecho al patrimonio en zona Lima Norte en el año 2023, segundo Identificación del estado de problema mediante la lectura de antecedentes y la experiencia en la realidad, tercero buscamos aportes nacionales e internacionales sobre el tema, cuarto determinación del problema de investigación, quinto hicimos la descripción del problema de la investigación, sexto creamos la formulación del problema y objetivos, séptimo constituimos la revisión y análisis de las teorías relacionadas al tema, octavo concebimos la categorización y subcategorización de las unidades de análisis al mismo instante hicimos las palabras claves, noveno creamos la estructuración de las metodologías aplicadas a la investigación, décimo formulamos la entrevista, undécimo formamos la elaboración de la discusión y resultados. Duodécimo paso hicimos las conclusiones y recomendaciones, por último, elaboramos el informe final de la investigación.

Finalmente, el documento del informe final la subimos en la plataforma trile de la Universidad Cesar Vallejo en rubro aula virtual alumno, en la sección productos de observación, para que lo revise el docente y la calificación de los jurados elegidos para este proceso, en donde dejan constancia de su veredicto, luego de la revisión del documento, posteriormente desarrolla la sustentación y la defensa de la investigación desarrollada por parte del investigador. Finalmente, este documento de tesis debe ser derivada y elevada en los recursos de consulta en la biblioteca del Universidad Cesar Vallejo.

Tabla 2: Trayectoria metodológica de la investigación

1. Exploración e identificación del problema	2. Identificación del estado de problema	3. Aportes nacionales e internacionales sobre el tema
4. Determinación del problema de investigación	5. Descripción del problema de la investigación	6. Formulación del problema y objetivos
7. Revisión y análisis de las teorías relacionadas al tema	8. Categorización y subcategorización de las unidades de análisis	9. Estructuración de las metodologías aplicadas a la investigación
10. La entrevista	11. Elaboración de la discusión y resultados	12. Conclusiones y recomendaciones
	13. Elaboración del informe final de la investigación	

3.7. Rigor científico: La firmeza científica se concibe que es coherente con la calidad de la investigación y la fiabilidad de los métodos empleados para obtener los resultados de la investigación. De manera que, afirma Chambi (2016), que los elementos del conocimiento de rigor científico son; **la exactitud, la precisión, la objetividad y la minuciosidad.** En este trabajo académico hemos realizado los elementos antes mencionados; de los cuales mana la rigurosidad de la encuesta, que se reflejó en la calidad moral, destrezas y experiencias sobre el tema. De esta manera, hemos evitado improvisaciones del argumento que se está discutiendo, por lo mismo que proporcionó una indagación plausible de la finalidad de la entrevista.

Como también, en el rigor científico; “[...]reconstrucciones teóricas [...] búsqueda de la coherencia entre las interpretaciones, es equivalente a la validez y la confiabilidad de la investigación cuantitativa, empleados para ello:

la dependencia o consistencia lógica, la credibilidad, la audibilidad, confiabilidad y la transferibilidad o aplicabilidad” (Hernández, Fernández y Baptista, 2010).

Nuestra investigación tiene consistencia **lógica** porque, nuestro raciocinio esta derivado de las premisas primigenias, no se aleja del tema a tratar, se logró la **credibilidad** ya que nuestra investigación está basado en la realidad palpable, también, nuestra investigación tiene la característica de la **audibilidad**, ya es fácilmente discernible, interpretable y entendible por todos, en cuanto a la **confiabilidad** lo que afirmamos se demuestra en otros lugares, nuestro trabajo de investigación es **aplicable y transferible** en diferentes otros contextos.

Mediante el rigor científico se aplica los pasos, procesos del método científico, la rigurosidad científica está contemplado el control de calidad de la investigación de un asunto o materia.

Tabla 3: Validación de Instrumento de la Guía de Entrevista

Validador	Cargo	Porcentaje	Condición
Mariano Rodolfo, Salas Quispe	Docente de la Universidad Cesar Vallejo	95%	Aceptable
Juan Carlos, Angulo Huaylupo	Docente de la Universidad Cesar Vallejo	95%	Aceptable
Ketty, Rojas Mayta	Docente de la Universidad Cesar Vallejo	95%	Aceptable

Fuente propio 2023

3.8. Método de análisis de datos: Hemos tratado un método conveniente para percibir, comprender y analizar la información lograda, de modo literal o narrativa, de contenidos análogos.

El método de análisis de información utilizado fue: En primer lugar, el hallazgo y la obtención de los datos relevantes, en segundo lugar, la elaboración, revisión y reproducción de los datos a textos, tercer lugar organizamos los datos como

cronológicos o temáticos e informativos, en cuarto lugar, categorizamos. Mediante el rotulado y clasificación de los datos, y por último analizaremos y generamos propuestas y conclusiones. Se utilizó el proceso de triangulación y cruzamiento de los datos mediante un cuadro de doble entrada.

Como menciona Charres (2018) “La triangulación intersubjetiva permite contrastar los diferentes puntos de vista que tienen los implicados sobre una misma realidad, en este caso los investigadores”. Es muy importante diferenciar las otras opiniones realistas de los expertos referente al tema que se está investigando.

Como también referente al método de análisis de información forma parte del proceso de adquisición y apropiación de los conocimientos que existen en las diferentes fuentes de información, así como las opiniones de los expertos (Sarday, 2007).

Teniendo en cuenta los términos referidos, resultado y discusión, procederemos a explayar la discusión de los fundamentos explicativos de los aportes de las especialistas entrevistadas. De las respuestas del guía de entrevista manejados para obtener aporte de los experimentados conocedores del contenido fraude informático y el derecho al patrimonio en Lima Norte 2023, como, fiscales, abogados penalista conocedores del delito informático, catedráticos universitarios en derecho penal y los peritos de la División de Investigación de Delitos de Alta Tecnología de la PNP (DIVINDAT). Fueron diferenciadas y verificadas con las fuentes académicas utilizadas, las tesis nacionales, locales e internacionales para lograr concebir la problemática explicado en la introducción, para ello se plantearon tres objetivos.

- 3.9. Aspectos éticos:** Hemos considerado la originalidad, la autenticidad y los aportes intelectuales. Como también, hemos respetado la propiedad intelectual y las opiniones de los autores de revistas, libros, tesis o cualquier material consultado. Si la transcribimos, como material de consulta para nuestra investigación, la hemos citado al autor de dicho material, postulado o asunto. Igualmente utilizamos las normas APA 7ª edición para las citas, considerando

el autor y año de investigación, en la realidad problemática, antecedentes y marco teórico.

A la par, nuestra materia de investigación fue contrastada con sumo cuidado utilizando software turnitin que nos arroja 10% de coincidencias, que equivale como norma técnica de aceptación para la Universidad Cesar Vallejo. Además, respetamos las normas éticas de la investigación como la **beneficencia**, equivale que nuestra investigación favorecerá en mejora de la convivencia social, de la misma forma, el trabajo de investigación tiene **autonomía**, es decir, independencia y transparencia, igualmente buscamos la **justicia** social y la tranquilidad de las personas naturales y/o jurídicas. A sí mismo, respetamos las directivas la normatividad de la Universidad Cesar Vallejo.

IV. RESULTADOS Y DISCUSIÓN

Referente a los **resultados**, se ha hecho la reproducción de las respuestas efectuadas a varios especialistas competentes en materia de delitos informáticos, mediante la técnica de la entrevista, utilizando como instrumento la guía de la entrevista. Las respuestas a estas entrevistas, así como los entrevistados están en el anexo de este trabajo de investigación.

Concerniente a la **discusión**, hemos hecho el comentario de las opiniones auténticas de los especialistas, a la luz de su conocimiento y manejo sobre el tema entrevistado, hemos dado elucidaciones legítimas y demostrativas proporcionando comentario de los fundamentos contruidos, con la encontramos semejanzas, discrepancias y concordancias (Mata,2020).

Tabla 3: Lista de documentos

N°	Autor	Año	País	Título	Fuente	Base de Datos	Objetivos
1	Mayer y Olivera	2020	Chile	El delito de fraude informático: concepto y delimitación	SciELO	https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842000100151&lang=es	Objetivo General
2	Chávez Rodríguez Elías Gilberto	2018	Perú	El Delito Contra Datos y Sistemas Informáticos en el Derecho Fundamental a la Intimidad Personal en la Corte Superior de Justicia de Lima Norte, 2017	repositorio.unfv.edu.pe	https://repositorio.unfv.edu.pe/bitstream/handle/20.500.13084/2704/CHAVEZ%20RODRIGUEZ%20ELIAS%20GILBERTO%20-%20DOCTORADO.pdf?sequence=1&isAllowed=y	Objetivo General
3	Tuesta Estela, Rosa Clara	2022	Perú	Fraude informático y su impacto en los derechos fundamentales de la persona en el Cercado de Lima – 2022	repositorio.uwiener.edu.pe	https://repositorio.uwiener.edu.pe/bitstream/handle/20.500.13053/8054/T061_46499897_TSP.pdf?sequence=1&isAllowed=y	Objetivo General
4	Peña Peña Milton Eduardo	2023	Colombia	Delitos Cibernéticos	repository.unilibre.edu.co	https://repository.unilibre.edu.co/bitstream/handle/10901/24774/TESIS%20VERSION%20APROBADA.pdf?sequence=1&isAllowed=y	Objetivo General
5	Vinelli Renzo Antonio	Vereau, 2021	Perú	Los delitos informáticos y su relación con la criminalidad económica	Alicia	https://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/4995	Objetivo General
6	Vences Oscar Manuel	Sánchez 2019	México	Penalización de los delitos informáticos	MEX - México	http://riaa.uaem.mx/xmlui/handle/20.500.12055/2675?show=full	Objetivo Especifico 1

7	Ancco Jacqueline	Pineda, 2022	Perú	El crimen organizado y su relación con la seguridad informática en Lima, año 2021	repositorio .ucv.edu.pe	https://repositorio.ucv.edu.pe/handle/20.500.12692/100567	Objetivo Especifico 1
8	Huamán Marleny Yudy	Cruz, 2020	Perú	Los delitos informáticos en Perú y la suscripción del Convenio de Budapest	repositorio .uandina.edu.pe	https://repositorio.uandina.edu.pe/handle/20.500.12557/4116	Objetivo Especifico 1
	Condori Ccori, Rufino	2020	Perú	Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020	repositorio .ucv.edu.pe	https://repositorio.ucv.edu.pe/handle/20.500.12692/63158	Objetivo Especifico 1
9	Dávila Rojas Melanio	Oscar 2018	Perú	EL DELITO CONTRA DATOS Y SISTEMAS INFORMÁTICOS EN EL DERECHO FUNDAMENTAL A LA INTIMIDAD PERSONAL EN LA CORTE SUPERIOR DE JUSTICIA DE LIMA NORTE, 2017	repositorio .unfv.edu.pe	http://repositorio.unfv.edu.pe/bitstream/handle/20.500.13084/2704/CHAVEZ%20RODRIGUEZ%20ELIAS%20GILBERTO%20-%20DOCTORADO.pdf?sequence=1&isAllowed=y	Objetivo Especifico 1
10	Condori Rufino	Ccori, 2020	Perú	Implicancias jurídicas del fraude informático y la protección penal del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020	repositorio .ucv.edu.pe	https://repositorio.ucv.edu.pe/handle/20.500.12692/63158	Objetivo Especifico 2
11	Morena del Río María	2020	Argentina	La importancia del bien jurídico tutelado en el ámbito de las sanciones administrativas con factor objetivo de atribución.	dialnet.unirioja.es	https://dialnet.unirioja.es/descarga/articulo/7792324.pdf	Objetivo Especifico 2
12	Collque casas Luis	José 2020	Perú	Lineamientos para La Aplicación de Evaluación Psicológica y Daño.	La Correcta es.scribd.com	https://es.scribd.com/document/449769780/LINEAMIENTOS-PARA-LA-CORRECTA-APLICACION-DE-LAS-GUIAS-DE-EVALUACION-PSICOLOGICA-Y-DANO	Objetivo Especifico 2

Fuente propia 2023

Relativo al primer objetivo de la presente indagación, es determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte. Los resultados de los magistrados especialistas entrevistados coinciden en que se

vulnera el derecho al patrimonio ante el fraude informático mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos. Afirman que se va incrementando el fraude informático con el avance la ciencia y la tecnología.

Por otro lado, en cuanto a la investigación y sanción en estos tipos de delincuentes en más compleja ya que lo hacen forma remota de lugares alejados utilizando el internet para cometer sus delitos, también afirman que muchos casos quedan indeterminados por la complejidad de elementos tecnológicos utilizados por los delincuentes, sobre todo por el borrado de pistas de información luego de cometido el fraude informático. Además, en los trabajos de investigación los autores que mencionaremos; Chávez (2018), Mayer y Oliver (2020), Tuesta (2020), Vinelli (2021), Peña (2023) han coincidido sobre el fraude informático como modalidad delictiva que va en aumento y que cada vez es más compleja. Que los delincuentes que cometen estos delitos son personas expertas en tecnologías de la información, siendo que tienen amplio conocimiento del manejo de redes y dispositivos informáticos, por lo que pueden obtener información hackeando cuentas de WhatsApp, Facebook o Instagram, como también, se cometen estos delitos cuando se roba o hurta un teléfono celular.

Como también, a nivel de marco teórico existen coincidencias de manera frecuentes con las perspectivas de los prosistas, Jiménez (2017), Espinoza (2022) y otros, que el fraude informático perjudica al patrimonio de las personas de manera creciente en las actuales circunstancias, causando daños económicos y psicológicas a las víctimas.

Referente al resultado obtenido de los especialistas entrevistados, adjuntamos un cuadro de doble entrada donde se visualiza las dos categorías del tema de investigación (Fraude Informático y derecho al patrimonio) y los objetivos tanto general como específicos, las nueve preguntas están plasmadas en la guía de la entrevista y las respuestas de los ocho expertos, de acuerdo a su experiencia y conocimiento sobre el tema, a continuación, presentamos una tabla de las respuestas de los entrevistados relativo al fraude informático y el derecho al patrimonio en Lima Norte 2023, el cuadro está estructurado de la siguiente manera: La Categoría, El objetivo. La pregunta y las respuestas de los 8 entrevistados.

Tabla 5: Respuesta de los entrevistado según las categorías

Categoría 1 – Fraude Informático		
Indicador	Preguntas	Respuestas
Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023	Pregunta 1: ¿Cómo vulnera el derecho al patrimonio ante un fraude informático?	<p>(E1) Se vulnera el derecho al patrimonio mediante la clonación de tarjetas, sustracción de claves y la transgresión de los aplicativos de los bancos en los celulares, entre otras.</p> <p>(E2) Las denuncias por el delito Contra el Patrimonio – Fraude Informático, con el pasar de los años se han venido incrementando de manera alarmante toda vez que a través de la tecnología los delincuentes de dotan de diversas herramientas para cometer los delitos especialmente a través de las redes, lo que hace más compleja la investigación para la Policía Nacional del Perú.</p> <p>(E3) Se vulnera mediante la, eliminación, supresión, modificación, de datos de los sistemas informáticos en sus distintas modalidades según la Ley N° 30096 que lo contempla.</p> <p>(E4) La finalidad en el fraude informático es obtener un beneficio económico, transfiriendo dinero de una persona a la cuenta del delincuente, con lo cual causa un perjuicio a la víctima, porque le están robando prácticamente su dinero, pero de manera virtual utilizando medios electrónicos.</p> <p>(E5) Debemos entender que el derecho al patrimonio es un derecho inescrutable. Pero ante los actos dolosos configurados en el tipo penal fraude informático, la integridad de un patrimonio se ve trasgredido.</p> <p>(E6) El derecho al patrimonio es un derecho inalienable, exclusivo, propia, sin embargo, ante los actos dolosos configurados en el tipo penal fraude informático, la integridad de un patrimonio se ve quebrantado, deshonrado y mancillado.</p> <p>(E7) Se vulnera mediante la alteración, supresión de sistemas informáticos en sus distintas modalidades de la Ley N° 30096 y sus modificatorias.</p> <p>(E8) Se vulnera realizando conductas previstas en la Ley de Delitos Informáticos N° 30096 y su modificatoria.</p>
	Pregunta 2: ¿Cuáles son las	<p>(E1) El vaciado del dinero de las cuentas bancarias y /o compras por internet de las personas naturales y/o jurídicas.</p> <p>(E2) En la actualidad todos los ciudadanos nos encontramos expuestos a ser víctima de este tipo de delitos, lo que genera inseguridad y falta de confianza al momento de confiar su dinero o sus ahorros en una entidad bancaria ya que están expuestos a que los delincuentes puedan clonar sus tarjetas o emplear hackers para vulnerar sus cuentas bancarias.</p>

<p>implicancias y consecuencias del delito del fraude informático?</p>	<p>(E3) Referente a las implicancias y consecuencias del delito de fraude informático, éstas se realizan investigaciones en la DIVINDAT y Fiscalía Especializada de la Ciberdelincuencia.</p> <p>(E4) Para la víctima es que va perder su patrimonio, lo cual le va causar gran afectación, por otro lado, si el delincuente y podrá ser reprimido con una pena privativa de la libertad no menor de 03 años, ni mayor de 8 años, y con 60 a 120 días multa.</p> <p>(E5) Las influencias y/o consecuencias son: i) Robo de información personal, ii) Reducción de patrimonio. Todo ello en perjuicio de los afectados.</p> <p>(E6) Las influencias y/o consecuencias son: a) Sustracción de información propia, b) Disminución de heredad o patrimonio. Todo ello en perjuicio de los afectados mediante el fraude informático.</p> <p>(E7) Dentro de las implicancias y consecuencias esta que se realizan investigaciones en la DIVINDAT y Fiscalía Especializada de la Ciberdelincuencia.</p> <p>(E8) La implicancia mediante la afectación patrimonial y afectación moral de las personas naturales y/o jurídicas. Consecuencias Fomenta la inseguridad ciudadana.</p>
<p>Pregunta 3: ¿Qué medidas o estrategias de investigación se debe aplicar referente al delito de fraude informático?</p>	<p>(E1) En las operaciones con tarjetas poner un monto mínimo de retiro de transferencias o compras por internet, si es posible pagar un seguro por pérdida o robo de las tarjetas de débito, crédito, si se mueve montos mayores.</p> <p>(E2) La PNP, al tomar conocimiento sobre un hecho ilícito en la modalidad de Fraude Informático, procede a poner de conocimiento de ministerio público, la noticia criminal a fin de que de manera coordinada pueda agotar los medios y emplear medios para la identificación y la posible detención del presunto autor o autores del hecho ilícito siempre y cuando se encuentre en flagrante delito; asimismo, se exhorta a los ciudadanos tener cuidado al momento de hacer uso de sus tarjetas bancarias y cuando hace retiro de dinero en las agencias y/o cajeros automáticos.</p> <p>(E3) Denuncias oportunas a la policía o fiscalías de delitos informáticos, pericias informáticas, para determinar el sistema usado, información a entidades bancarias en caso de fraude informático.</p> <p>(E4) Estos delitos deben ser investigados por servidores y funcionarios públicos debidamente capacitados y que cuenten con las herramientas tecnológicas para poder realizar de manera correcta una investigación, siendo que es necesario que la Unidad Fiscal Especializada en Ciberdelincuencia lleve estos casos.</p> <p>(E5) Las medidas a tomar son: i) Protección de nuestra información, ii) Tener claves o contraseñas seguros, iii) No proporcionar los datos sin considerar la seguridad del receptor.</p>

		<p>(E6) Especialización en fraude informático nivel de fiscalías, jueces, operadores de justicia y la DIVINDAT- PNP. Y la información a la ciudadanía sobre la protección de sus datos de manera segura, uso de redes sociales adecuadamente.</p>
		<p>(E7) Reportar la pérdida o robo de las tarjetas y/o dispositivo móvil para el bloqueo. Denuncias oportunas a la policía o fiscalías de delitos informáticos. Pericias informáticas, para determinar el sistema usado información a entidades bancarias en caso de fraude informático.</p>
<p>Objetivo2 Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023</p>	<p>Pregunta 4: ¿Cómo cree usted que los delincuentes obtienen datos ilegales para ejecutar el delito de fraude informático?</p>	<p>(E8) Especialización en materia de ciberdelincuencia nivel de fiscalías, jueces, operadores de justicia y la División de Investigación de Delitos de Alta Tecnología de la PNP (DIVINDAT-PNP).</p> <hr/> <p>(E1) En los centros nocturnos donde hay ingesta de bebidas alcohólicas, utilizando a bellas féminas, para que ellas roben sus claves secretas, tejas de créditos y/o débito, celulares, etc. Mediante la modalidad de pepeo.</p> <hr/> <p>(E2) Generalmente los delincuentes usan nuestra propia información lo cual obtienen a través de llamadas telefónicas, mensajes de texto o mensajes de WhatsApp donde se hacen pasar por asesores bancarios ofreciendo préstamos o facilidades para obtener tarjetas bancarias para lo cual solicitan brinden información estrictamente confidencial como número de tarjetas y clave secreta.</p> <hr/> <p>(E3) Mediante la suplantación de identidad, valiéndose de llamadas y/o mensajes simuladas, clonación de tarjetas robadas.</p> <hr/> <p>(E4) Los delincuentes son personas expertas en tecnologías de la información, por lo que pueden obtener información hackeando cuentas de WhatsApp, Facebook o Instagram, además también se cometen estos delitos cuando se roba o hurta un teléfono celular.</p> <hr/> <p>(E5) Hoy en día acceder a la base de datos informacional de las personas naturales y/o jurídicas es muy sencillo de adherirse, existen lugares donde por un robo te obtienen esta información. Ejemplo centro comercial de Wilson.</p> <hr/> <p>(E6) Utilizando expertos en cibernética, ingresando a base de datos vulnerando, archivos en el sistema financiero y comercial, mediante el quebrantamiento de datos personales o claves secretas de las personas naturales y/lo jurídicas.</p> <hr/> <p>(E7) Mediante la suplantación de identidad, valiéndose de llamadas simuladas, simulando ofertas y/o regalos de una entidad benéfica.</p> <hr/> <p>(E8) A través de ataques cibernéticos por los hackers, la vulneración de los archivos en el sistema financiero y el quebrantamiento de datos personales o claves secretas de las personas naturales y/lo jurídicas.</p>

<p>Objetivo2 Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023</p>	<p>Pregunta 5: ¿Considera usted que la fiscalía conjuntamente con la alta dirección de tecnología de PNP se encuentra capacitada para afrontar el delito de fraude informático?</p>	<p>(E1) Si, se encuentra capacitado, siempre en cuando los agraviados denuncien oportunamente estos hechos, la PNP está en la capacidad de enfrentar los delitos de fraude informático y otros delitos cibernéticos.</p> <p>(E2) La modalidad del delito de fraude informativo es un tipo penal nuevo, tanto el ministerio público, así como la policía nacional vienen realizando esfuerzos para combatir ese tipo de ilícitos; sin embargo, no es suficiente el esfuerzo o empeño que acarrea realizar dicha investigación ya que se necesita de medios tecnológicos y herramientas sofisticadas para detectar e identificar a los presuntos responsables de los delitos ya mencionados.</p> <p>(E3) Si, ya que existen unidades especializadas como son la DIVINDAT y la fiscalía de la ciberdelincuencia, que están trabajando referente a delitos informáticos en caso de fraude informático.</p> <p>(E4) La Unidad Fiscal Especializada en Ciberdelincuencia de Lima cuenta con un laboratorio tecnológico, personal de apoyo (ingenieros de sistemas), servidores y funcionarios públicos capacitados para realizar investigación sobre el delito de fraude informático y otros delitos informáticos.</p> <p>(E5) Considero que sí, aunque, con el avance vertiginoso de la informática, las fiscalías especializadas en delitos cibernéticos, y la DIVINDAT de la PNP deben capacitarse constantemente.</p> <p>(E6) Considero que sí, aunque, con el avance acelerado del tratamiento de la información, las fiscalías especializadas en delitos cibernéticos, y la DIVINDAT de la PNP deben capacitarse constantemente.</p> <p>(E7) Si, ya que existen unidades especializadas como son la DIVINDAT y la fiscalía de la ciberdelincuencia, enfrenta los delitos de fraude informático y otros delitos Cibernéticos.</p> <p>(E8) En la actualidad falta mayor capacitación y dotación de herramientas tecnológicas para combatir el delito de fraude informático y otros delitos que se cometen utilizando internet o clonando tarjetas perdidas.</p>
<p>Objetivo2 Determinar la manera que se</p>	<p>Pregunta 6: El que deliberada e ilegítimamente [...] manipula un sistema</p>	<p>(E1) Ya que este es el modo operandi de personas de dudosa reputación, que se debe doblar la pena de 12 a 25 años de pena privativa de libertad, sin beneficios carcelarios.</p> <p>(E2) La modalidad del delito de fraude informativo es un tipo penal nuevo, tanto el ministerio público, así como la policía nacional vienen realizando esfuerzos para combatir ese tipo de ilícitos; sin embargo, no es suficiente el esfuerzo o empeño que acarrea realizar dicha investigación ya que se necesita de medios tecnológicos y herramientas sofisticadas para detectar e identificar a los presuntos responsables de los delitos ya mencionados.</p>

accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023	a informático, será reprimido con una pena privativa de libertad no menor de 3 ni mayor de 8 años”; las penas son suficientes para	(E3) Las penas no son suficientes de 3 y 8 años, corre la posibilidad que dicha pena sea suspendida de libertad y que el autor sea citado e investigado en su domicilio, de donde puede seguir delinquiendo y lo puede realizar a través de la tecnología, empleando una computadora, laptop, aparatos móviles o cualquier aparato electrónico que le puede ser útil.
	salvaguardar a las personas en la sociedad ante el fraude informático?	(E4) Si, en base al principio de proporcionalidad en sentido estricto y las penas deben ser mayores desde 8 años a 20 años de pena privativa de libertad, sin beneficios carcelarios, de acuerdo a la gravedad del delito.
		(E5) Considero que la pena debe aumentar, debería ser una pena no menor de 04 ni mayor de 08 años, para que la pena que se dicte sea efectiva y no suspendida, ya que de sus casas siguen cometiendo el delito.
		(E6) Considero que las penas privativas de libertad deben estar en proporción a la infracción cometida por el sujeto activo. En ese sentido deben aumentar la pena.
		(E7) Las penas privativas de libertad deben estar en proporción a la infracción cometida por el sujeto activo. En ese sentido deben aumentar la pena, de 5 a 10 años. Para que la pena sea efectiva.
		(E8) Un mayor incremento de la pena no garantiza, es necesario políticas de prevención, información adecuada a la ciudadanía, equipamiento y capacitación al DIVINDAT de la PNP, a los fiscales, jueces y operadores de justicia.

Categoría 2 – Derecho al patrimonio

Objetivo 3 Identificar los daños materiales y morales que ocasionan el fraude informático con la	Pregunta 7: ¿Considera usted, que ante la comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado	(E1) Si se agravia la totalidad de las cuentas bancarias y / o mercaderías con compras por internet, mediante la usurpación de la propiedad privada.
		(E2) Si, se vulnera el derecho al patrimonio, ya que queda impune debido a que no se logra dar con el paradero de los autores del hecho, si es que el usuario no paga un seguro contra robo en la entidad bancaria es casi imposible que pueda recuperar su dinero.
		(E3) Si se vulnera el derecho al patrimonio cuando se roba el secreto de los datos propios del patrimonio protegido por la ley y los derechos fundamentales.
		(E4) Considero que sí, porque se puede transferir dinero a la cuenta del delincuente, afectando el patrimonio de la víctima.
		(E5) Si, debido a que es una disminución de patrimonio, por lo que le genera pérdidas al sujeto afectado por el fraude informático.

vulneración a nuestro patrimonio en Lima Norte 2023	pérdida material?	<p>(E6) Si, afecta la comisión de fraude informático al vulnerar el derecho al patrimonio, mediante la pérdida del patrimonio del sujeto perjudicado por el fraude informático.</p> <p>(E7) Si se vulnera el derecho al patrimonio; pero no se vulnera el derecho a la información mediante los delitos informáticos.</p> <p>(E8) La comisión de fraude informático si, afecta primordialmente al patrimonio neto de las personas naturales y/o jurídicas.</p>
---	-------------------	--

<p>Pregunta 8: ¿Considera usted, que ante comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado daño moral?</p>	<p>(E1) Si en el fraude informático se ocasiona a el daño moral: porque tendrán que empezar de nuevo, ya que dejan las cuentas en 0, por esta razón las personas sufren tristeza y depresión.</p> <p>(E2) Definitivamente afecta el daño moral ya que al momento que ser afectado el bien patrimonial el agraviado entra en un estado depresivo y de incertidumbre al no saber cómo se pudo generar dicha acción.</p> <p>(E3) Sufren trastornos emocionales. desespero, angustia, inseguridad económica y perturbaciones fisiológicos en general.</p> <p>(E4) Considero que sí, porque al perder su patrimonio monetario, las victimas pueden deprimirse por ver frustrados sus proyectos que tenían planeados.</p> <p>(E5) Se debe entender por daño moral a la afectación de una acción que causa angustia o sufrimiento. El cual debe resarcirse. el ser afectado emocionalmente, debe conllevar a una compensación.</p> <p>(E6) Entendido el daño moral a la acción que causa pena, angustia o sufrimiento. El cual debe repararse. El ser afectado emocionalmente, debe ser sujeto a una compensación económica por parte del sujeto activo.</p> <p>(E7) Sí, pero muchas veces en caso de delitos fraude informático se ve la imposibilidad de obtener y recuperar su patrimonio causando daño psicológico.</p> <p>(E8) La comisión de fraude informático, si vulnera teniendo como resultado el daño moral, que consiste en la preocupación, ansiedad, desorden fisiológico, como náuseas, palpitaciones, irritabilidad.</p>
--	--

<p>Pregunta 9: ¿Se compensa completamente el daño moral ocasionado en</p>	<p>(E1) Si, se debe compensar el daño moral, siempre en cuando se identifica al culpable, o la persona que perpetró el delito de fraude informático.</p> <p>(E2) Al ser víctima del delito contra el patrimonio – Fraude Informático, la persona agraviada ya no vuelve a recuperar la confianza ya que la afectación emocional es evidente y así recupere su patrimonio</p>
--	--

el delito siempre queda una inseguridad al momento de realizar una transacción informático? bancaria.

(E3) No, se puede compensar el daño moral, debido a que, en el delito de fraude informático, no se puede identificar a los autores, dado la modalidad delictiva empleada, ya muchas veces se cometen desde lugares alejados, otros países. Departamentos alejados, hasta de la prisión.

(E4) Considero que no, porque las victimas generalmente quedan afectadas moralmente por haber sufrido esta situación.

(E5) No, debido a que no se puede medir el daño moral en ese sentido los delitos informáticos se ajustan a sus efectos.

(E6) No se compensa el daño moral ocasionado en el delito informático, ya que no se puede acreditar el hecho afectado moralmente que se ajusten a sus efectos.

(E7) No, se puede compensar completamente el daño moral, debido a que, en muchos casos en el delito de fraude informático, no se puede identificar a los autores, dado la modalidad delictiva empleada.

(E8) Muchas veces no se compensa el daño moral ocasionado en el delito informático, ya que no se puede acreditar el hecho afectado.

Pregunta 10: ¿Qué opinión le gustaría compartir en relación a la presente investigación?

(E1) En nuestro país las Leyes son muy benignas para cierto tipo de delitos informáticos. Hay personas que les dejan en ruina total y que se debía legislar para que dichas penas sean más drásticas.

(E2) Es necesario realizar modificatorias en la norma que sanciona el Fraude Informático, de todos los presupuestos establecidos, con una pena privativa de libertad. Asimismo, el gobierno debe dotar de material tecnológico avanzado para la investigación de hechos.

(E3) Dotar de mayor capacitación del personal del DIVINDAT - PNP, Jueces, fiscales y operadores jurídicos y mayor presupuesto para equipamiento con alta tecnología para la identificación, detección, juzgamiento y sanción de autores del delito de fraude informático.

(E4) Considero que el tema de tesis es interesante e importante, necesitamos mayores aportes para mejorar esta modalidad de delito.

(E5) Concluyó que la investigación, aporta nuevas nociones e ideas que las autoridades competentes deben considerar al tratar este delito y por otro lado los sujetos afectados deben tomar las precauciones y/o contingencias al respecto.

(E6) Recomendamos denunciar hechos de robo de celulares, tarjetas de créditos, débitos y a las llamas anónimas amenazadoras al celular N° 942 440 729 o al correo electrónico divindat.servicioguardia@policia.gob.pe.

(E7) Que en la actualidad la DIVINDAT-DIRINCRI, se encuentran saturadas en las pericias informáticas que se suelen requerir de los medios y dispositivos usados.

(E8) Que se tenga en cuenta la Ley N° 30096 y la observancia de casos fiscales sobre ciberdelincuencia que está a disposición y de acceso del público. Denunciar el robo de celulares, tarjetas al celular N° 942 440 729 o al divindat.servicioguardia@policia.gob.pe.

Análisis de las respuestas de los expertos entrevistados:

Categoría 1.- Fraude Informatico.

Objetivo General: Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023. Con la **Pregunta 1:** ¿Cómo se vulnera el derecho al patrimonio ante un fraude informático? La respuesta predominante fue Se vulnera mediante la, eliminación, supresión, modificación, de datos de los sistemas informáticos en sus distintas modalidades según la Ley N° 30096 que lo contempla, mediante uso de celulares y clonación de tarjetas. Respecto a la **Pregunta 2:** ¿Cuáles son las implicancias y consecuencias del delito del fraude informático? El retiro no autorizado del dinero de las entidades bancarias y finieras, utilizando el internet y la compra de productos, con tarjetas clonadas de los centros comerciales. En la **Pregunta 3:** ¿Qué medidas o estrategias de investigación se debe aplicar referente al delito de fraude informático? 1ro. Bloqueo de tarjetas perdidas y/o del celular, 2do. Denunciar el hecho en la comisaria o ministerio público, conservando el historial de acciones anteriores al hecho. 3ro. Para la PNP y fiscalías especializadas en delitos informático, cumplir los protocolos de proceso.

Objetivo específico 1.- Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023, **Pregunta 4:** ¿Cómo cree usted que los delincuentes obtienen datos ilegales para ejecutar el delito de fraude informático? 1ro. Mediante llamadas telefónicas o mensajes de textos utilizando; Messenger, WhatsApp, Facebook, Instagram, 2do. Mediante sustracción de celulares y/o tarjetas de crédito o débito, 3ro. Mediante la clonación de tarjetas de crédito y/o débito. 4to. Mediante suplantación de identidad utilizando indigentes como personas favorecidas. 5to. Descifrando clandestinamente los claves secretos. **Pregunta 5:** ¿Considera usted que la fiscalía conjuntamente con la alta dirección de tecnología de PNP se encuentra capacitada para afrontar el delito de fraude informático? Si, mediante denuncia oportuna ante la División de

Investigación de Delitos de Alta Tecnología (DIVINDAT) de la PNP y la Fiscalía Especializada en Delitos Informáticos. Necesidad de dotación de equipos tecnológicos y capacitación de personal, **Pregunta 6:** “El que deliberada e ilegítimamente [...] manipula un sistema informático, será reprimido con una pena privativa de libertad no menor de 3 ni mayor de 8 años”; ¿Las penas son suficientes para salvaguardar a las personas en la sociedad ante el fraude informático? Si de aumentar la pena de 12 a 25 años de pena privativa de libertad sin beneficios carcelarios. Mayor difusión y prevención del delito.

Categoría2.- Derecho al Patrimonio.

Objetivo específico 2: Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023. **Pregunta 7:** ¿Considera usted, que ante la comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado pérdida material? Si, afecta la comisión de fraude informático al vulnerar el derecho al patrimonio, primordialmente mediante la pérdida del patrimonio del sujeto perjudicado por el fraude informático, **Pregunta 8:** ¿Considera usted, que ante comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado daño moral? Si en el fraude informático se ocasiona a el daño moral: porque tendrán que empezar de nuevo, ya que dejan las cuentas en cero, por esta razón el agraviado entra en un estado depresivo y de incertidumbre al no saber cómo se pudo generar dicha acción. Sufren trastornos emocionales. desespero, angustia, inseguridad económica y perturbaciones fisiológicos en genera. **Pregunta 9:** ¿Se compensa completamente el daño moral ocasionado en el delito informático? No, se puede compensar el daño moral, debido a que, en el delito de fraude informático, no se puede medir, precisar, acreditar el hecho afectado el daño moral, peor aún si no se puede identificar a los autores, debido que la modalidad delictiva empleada, se cometen desde lugares alejados, otros países, hasta de la prisión.

Igualmente, afirman los expertos encuestados que, la Unidad Fiscal Especializada en Ciberdelincuencia de Lima cuenta con un laboratorio tecnológico, personal de apoyo (ingenieros de sistemas), servidores y funcionarios públicos debidamente capacitados para poder realizar una correcta investigación, sobre el

delito de fraude informático y como también, de otros delitos informáticos; conconsideran que la pena privativa de libertad debe aumentar, debería ser una pena no menor de 04 ni mayor de 08 años, para que la pena privativa de libertad, que se sentencie sea efectiva y no suspendida.

En cuanto al segundo objetivo Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023, los encuestados coinciden en que sí, se puede transferir dinero a la cuenta del delincuente, afectando el patrimonio de la víctima, a si también se afecta psicológicamente porque al perder su patrimonio monetario, las victimas pueden deprimirse por ver frustrados sus proyectos que tenían planeados.

Referente al tercer objetivo Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023. Afirman los entrevistados que sí, existe daño material y moral porque al perder su patrimonio monetario, las victimas pueden deprimirse por ver frustrados sus proyectos que tenían planeados. A sí mismo, consideran que no se puede resarcir el daño moral, por la complejidad del delito y no se pude determinar frecuente al causante del delito, por lo tanto, las victimas generalmente quedan afectadas moralmente por haber sufrido esta situación y desamparado de este tipo de reparación.

Respecto a las respuestas de los expertos entrevistados referente a la **categoría Fraude Informático** afirman; se cometen fraude informático; obteniendo un beneficio económico, transfiriendo dinero de una persona a la cuenta del delincuente, de manera virtual utilizando medios electrónicos con lo cual causa un perjuicio a la víctima. Como también, la consecuencia para la víctima es que va perder su patrimonio monetario, lo cual le causará gran afectación para su vida; el delincuente podrá ser reprimido con una pena privativa de la libertad no menor de 03 años, ni mayor de 8 años, y con 60 a 120 días multa. A sí mismo, estos delitos deben ser investigados por servidores y funcionarios públicos debidamente capacitados y que cuenten con las herramientas tecnológicas para poder realizar de manera correcta una investigación, siendo que es necesario que la Unidad Fiscal Especializada en Ciberdelincuencia lleve estos casos. Por otro lado, se comete delitos de fraude informático, realizando conductas previstas en la ley 30096, Suplantación de identidad, uso de damas de

compañía para apropiarse de las tarjetas de débito y/o crédito, como también observándose, falta de mayor capacitación y dotación de tecnología a los policías de alta tecnología, fiscales, jueces y operadores jurídicos y se recomienda incrementar la pena de 12 a 25 años de pena privativa de libertad sin beneficios tributarios. Paralelamente se debe incrementar la prevención e información hacia el usuario.

Como también en cuanto a la entrevista realizada referente a la **categoría derecho al patrimonio** los especialistas responden coincidentemente que; si se vulnera el derecho al patrimonio cuando se afecta la privacidad del patrimonio de las personas naturales y/o jurídicas, de sus bienes muebles e inmuebles, habitualmente monetarias. Como también, frente a la imposibilidad de recuperar el patrimonio perdido, sufre la persona de daño psicológico o moral, se manifiesta mediante trastornos emocionales, desespero, angustia, inseguridad, ansiedad, entre otros. Asimismo, No se puede compensar completamente el daño moral, ya que es difícil de determinar la magnitud del daño, como también, al no poder identificar plenamente los autores del delito por la modalidad empleada.

Tabla 5: Resumen de coincidencias y discrepancias entre los entrevistados.

Categoría de entrevistado.	Coincidencias	Discrepancias
E-01 (PNP Experto en D.I.)	Por la alteración de las conductas previstas en la ley N° 30096. Aprovechamiento de la Informática y el internet en forma física y/o virtual.	El Fraude Informático se cometen por las redes sociales y el WhatsApp.
E-02 (PNP Experto en D.I.)	El vaciado de dinero de las cuentas bancarios y el robo mediante la modalidad de compra con tarjetas comerciales clonadas.	En la modalidad delito informático SKIMMING con skimmer, se copian los códigos de las tarjetas.
E-03 (Abogado Penalista).	La medidas o estrategias que se debe aplicar referente a delito de Reportar inmediatamente y dar facilidades para la búsqueda de posibles autores y la modalidad utilizada.	La medidas o estrategias que Capacitación e la PNP, fiscales, jueces y operadores jurídicos. y poner montos mínimos en retiro, transferencia, compras por internet.
E-04 (Abogado Penalista).	Utilizan expertos hoques para cometer el delito de fraude informático,	En los centros nocturnos, utilizando a bellas féminas, para que ellas roben sus claves secretas, tarjetas de créditos y/o débito.
E-05 (catedrático en Derecho Penal)	Considero que sí, aunque, con el avance vertiginoso de la informática, las fiscalías especializadas en delitos	Recitamos mayor capacitación de los jueces, fiscales y PNP y la DIVINDAT en el delito Fraude informático.,

		cibernéticos, y la DIVINDAT de la PNP deben capacitarse constantemente.	
E-06 (catedrático en Derecho Penal)		Si, ya que existen unidades especializadas como son la DIVINDAT y la fiscalía de la ciberdelincuencia, que están trabajando referente a delitos informáticos en caso de fraude informático.	Falta capacitar unidades especializadas como son la DIVINDAT y la fiscalía de la ciberdelincuencia, que están trabajando referente a delitos informáticos en caso de fraude informático
E-07 (Fiscal: Ministerio Público)		Si se vulnera el derecho al patrimonio cuando se roba el secreto de los datos propios del patrimonio protegido por la ley y los derechos fundamentales.	No se vulnera el derecho al patrimonio cuando se roba el secreto de los datos propios.
E-08 (Fiscal: Ministerio Público)		No, se puede compensar completamente el daño moral, debido a que, en muchos casos en el delito de fraude informático, no se puede identificar a los autores, dado la modalidad delictiva empleada	Si es factible resarcir el daño moral, psicológico del sujeto pasivo, cuando se denuncia inmediatamente y se captura al culpable.

Fuente propia 2023

Las coincidencias: El fraude informático se da por la alteración de las conductas previstas en la ley N° 30096. Aprovechamiento de la Informática y el internet en forma física y/o virtual y por el vaciado de dinero de las cuentas bancarios y el robo mediante la modalidad de compra con tarjetas comerciales clonadas. Éstas, debe ser reportado inmediatamente y dar facilidades para la búsqueda de posibles autores y la modalidad utilizada; cuanto a la fiscalía deben utilizar expertos para determinar el delito y condenar al delincuente.

Las penas privativas de libertad deben incrementarse sin beneficios carcelarios. No se recomienda prisión suspendida ya que fácilmente pueden cometer fraude de su domicilio.

Coinciden en la capacitación constante en esta modalidad de delitos, las fiscalías especializadas en delitos cibernéticos, y la DIVINDAT de la PNP por motivo del avance vertiginoso de la informática.

No, se puede compensar completamente el daño moral, debido a que, en muchos casos en el delito de fraude informático, no se puede identificar a los autores, dado la modalidad delictiva empleada

Las discrepancias son: La medida de subir sanciones no soluciona el delito informático, se requiere de estrategias integrales para erradicar este flagelo.

Si es factible resarcir el daño moral, psicológico del sujeto pasivo, cuando se denuncia inmediatamente y se captura al culpable.

V. CONCLUSIONES

Primera: En el delito de fraude informático se vulnera el derecho al patrimonio ante el fraude informático mediante el diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos, la investigación y sanción en estos tipos de delitos es más compleja, ya que lo hacen forma remota de lugares alejados, y muchos casos quedan indeterminados por la complejidad de elementos tecnológicos utilizados por los delincuentes, obtienen información hackeando cuentas de WhatsApp, Facebook o Instagram y también mediante el robo o hurto de un teléfono celular y/o tarjetas de crédito o débito.

Segunda: La manera que los delincuentes acceden a nuestras cuentas para adherirse a la información privada son diversas, como la clonación de tarjetas ,transferencias electrónicas fraudulentas, como la suplantación de identidad con personas discapacitadas o menores de edad, uso de damas de compañía en lugares donde se liba licores, así como en discotecas, bares, entre otras, para apropiarse del celular, de las tarjetas de débito y/o crédito, luego transfieren dinero de la cuenta de personas naturales y jurídicas, afectando el patrimonio de la víctima y la utilización de las principales modalidades ciberdelictivas; phishing, vishing, smishing, carding, skimming, pharming, ransomware.

Tercera: Luego de sufrir el robo mediante el delito de fraude informático, las víctimas son afectados moral y psicológicamente, presentando cuadros deprimentes de frustración, de baja de autoestima, palpitaciones, iras, rabia, cólera, desespero, intranquilidad cuando son frustrados sus proyectos que tenían planeados. No se puede resarcir el daño moral, por la complejidad del delito, ya que no se pudo determinar con frecuencia al causante del delito, por lo tanto, las víctimas generalmente quedan desalmadas económica y moralmente por haber preexistido como víctima del fraude informático.

VI. RECOMENDACIONES

Primera: Se recomienda capacitación constante del personal del DIVINDAT - PNP, Jueces, fiscales y operadores jurídicos y mayor presupuesto para equipamiento con alta tecnología para la identificación, detección, juzgamiento y sanción de autores del delito de fraude informático, y sobre todo el uso adecuado de los protocolos de seguridad de equipos incautados en el traslado y custodia de los mismos.

Segunda: Se recomienda incrementar la pena por cometer fraude informático de 12 a 25 años de pena privativa de libertad sin beneficios carcelarios, según la gravedad del delito y la cuantía del monto afectado, paralelamente se debe aumentar la prevención frente a este tipo de delito e incrementar la información masivamente utilizando los medios de comunicación intensiva hacia toda la población y se sugiere hacer compras digitales en páginas web conocidas , no responder a correos electrónicos o mensajes de textos donde nos pida información personal detallada, tener los archivos en un disco duro externo y utilizar programas y antivirus originales.

Tercera: Se recomienda de manera Inmediata cuando sucede el robo pérdida de un celular, lo primero que debemos hacer es bloquear el chip de móvil, lo mismo con las tarjetas de débito o crédito, sean bancarias o comerciales, es muy recomendable comunicar de manera rápida a las entidades bancarias o comerciales que son dadores de estas tarjetas; luego debemos apersonarnos a la comisaría de su jurisdicción para hacer la denuncia o ante un ministerio público más cercano al lugar de los hechos y Denunciar el robo de celulares, tarjetas de crédito o débito, al celular N° 942 440 729 y/o al correo electrónico: divindat.servicioguardia@policia.gob.pe .

REFERENCIAS

- Águila, E. (2019). Suplantación de la identidad digital con fines trata de personas en Facebook. Centro de investigación e innovación en tecnología de la información y comunicación, [propuesta de tesis para obtener el grado de maestro en derecho de las tecnologías de la información de la comunicación].
- Ancco, J. (2022). El crimen organizado y su relación con la seguridad informática en Lima, año 2021. <https://repositorio.ucv.edu.pe/handle/20.500.12692/100567>.
- Arias, J, L. (2021). Técnicas e Instrumentos de Investigación Científica. [file:///E:/AriasGonzales_TecnicasElInstrumentosDeInvestigacion_libro%20\(1\).pdf](file:///E:/AriasGonzales_TecnicasElInstrumentosDeInvestigacion_libro%20(1).pdf)
- Arias, L. A. (2021). "Limitaciones del sistema penal para investigar y probar la comisión del Ciberdelito en El Salvador. <https://ri.ues.edu.sv/id/eprint/26913/1/Limitaciones%20del%20sistema%20penal%20para%20investigar%20y%20probar%20la%20comisi%C3%B3n%20del%20Ciberdelito%20en%20El%20Salvador.pdf>.
- Aubry y Rau. (1963). El Patrimonio. <https://blogdeantuan.wordpress.com/2013/08/20/aubry-y-rau-el-patrimonio/>
- Azaola, L. (2017). Delitos informáticos y derecho penal. Editorial UBIJUS. Primera edición.
- Bokovnya (2020) , Legal Approaches to Artificial Intelligence Concept and Essence Definition. <https://revista.sangregorio.edu.ec/index.php/REVISTASANGREGORIO/article/view/1489/18-YRIEVNA>
- BID-OEA. (2020). Reporte Ciberseguridad. Riesgos, avances y el camino a seguir en América Latina y El Caribe. <https://publications.iadb.org/es/Reporte-ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-america-latina-y-el-caribe>.
- Blossiers, J. (2018). El Delito Informático Y Su Incidencia En La Empresa Bancaria. <https://www.congreso.gob.pe/Docs/comisiones/2020/CE-TribunalConstitucional/files/postulantes/exp037/tesis.pdf>
- Condori, R. (2020). Implicancias jurídicas del fraude informático y la protección penal

- del delito contra el patrimonio Distrito Fiscal de Lima Norte 2020. <https://repositorio.ucv.edu.pe/handle/20.500.12692/63158>.
- Collque, J. L. (2020). Lineamientos para La Correcta Aplicación de Las Guías de Evaluación Psicológica y Daño. <https://es.scribd.com/document/449769780/LINEAMIENTOS-PARA-LA-CORRECTA-APLICACION-DE-LAS-GUIAS-DE-EVALUACION-PSICOLOGICA-Y-DANO>
- Charres, H., Villalaz, J. & Martínez, J. (2018). Triangulación: Una herramienta adecuada para las investigaciones en las ciencias administrativas y contables. <http://portal.amelica.org/ameli/jatsRepo/221/2211026002/index.html>.
- Chávez, J. (2018). El Delito Contra Datos y Sistemas Informáticos en el Derecho Fundamental a la Intimidad Personal en la Corte Superior de Justicia de Lima Norte, 2017 (Tesis para abogado, UNFV). <https://repositorio.unfv.edu.pe/bitstream/handle/20.500.13084/2704/CHAVEZ%20RODRIGUEZ%20ELIAS%20GILBERTO%20-%20DOCTORA%20DO.pdf?sequence=1&isAllowed=y>
- Chero, F.I. (2022). Ciberdelincuencia reporte de información estadística y recomendaciones para la prevención. MJDH. <https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf.pdf>.
- Dulzaides, M. (2002). Análisis documental y de información: dos componentes de un mismo proceso. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1024-94352004000200011.
- El peruano (17 de septiembre, 2023). Sepa cómo evitar ser víctima de un delito informático. <https://www.elperuano.pe/noticia/204416-sepa-como-evitar-ser-victima-de-un-delito-informatico#:~:text=En%20el%20Per%C3%BA%20se%20registran,la%20Polic%C3%ADa%20Nacional%20del%20Per%C3%BA>.
- Espinoza, V. R. (2022). Delito Informáticos y Nuevas Modalidades Delictivas. Editorial Instituto Pacífico. Lima. Perú.
- Fuentes, K, (2021). Modificación de la ley 30096 para Incorporar los delitos de phishing, Pharming y carding como delitos Penalizados con prisión, para reducir La ciberdelincuencia, lima 2019. <https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/8345/Fuentes%20Garrido>,

- %20Karla%20Vanessa.pdf?sequence=1.
- Fuster, D. (2019). Investigación cualitativa: Método fenomenológico hermenéutico. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2307-79992019000100010
- Fernández, W; Vargas, C. (2018) ¿Son útiles las TIC para combatir la ciberdelincuencia? La relación entre la denuncia de delitos informáticos y el equipamiento tecnológico de las comisarías. *The Law, State and Telecommunications Review*, Brasilia, v. 10, n. 2, p. 37-52, October 2018. [DOI: <https://doi.org/10.26512/lstr.v10i2.21492>]
- Goñi, J.E. (2021) El cibercrimen en las transacciones con criptomonedas. (Tesis para obtener el título profesional de abogado- UCV) Lima Metropolitana. 2020 https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/79208/Go%C3%B1i_RJE-SD.pdf?sequence=1&isAllowed=y
- Huamán, M. (2020) los delitos informáticos en Perú y la suscripción del convenio de Budapest. <https://repositorio.uandina.edu.pe/handle/20.500.12557/4116>
- Jimenez (2017). Derecho Penal Informatico. Editorial Instituto Pacifico S.A.C. Perú.
- Landa, C. (2017). Derechos Fundamentals. <https://repositorio.pucp.edu.pe/index/bitstream/handle/123456789/170363/Los%20derechos%20fundamentales.pdf>
- Lanzito, C. (2023). Las estafas dejaron pérdidas récord de \$8,800 millones en 2022. <https://www.aarp.org/espanol/dinero/estafas-y-fraudes/info-2023/ftc-perdida-spor-delincuencia-2022.html>.
- Mata, L.D. (2020). La técnica cualitativa grupo focal o grupo discusión. <https://investigaliacr.com/investigacion/la-tecnica-cualitativa-grupo-focal-o-grupo-discusion/>.
- Martins, B, (2022) Convenio de Budapest sobre la ciberdelincuencia en América Latina. <file:///C:/Users/ANTINOGENES/Documents/ESP-Ciberdelincuencia2022.pdf>
- Mayer, L. y Olivera, G. (2020). El delito de fraude informático: concepto y delimitación. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842020000100151&lang=es
- Medardo, V. y Nizama, L. (2020). El enfoque cualitativo en la investigación jurídica,

- proyecto de investigación cualitativa y seminario de tesis. Vox juris 38.2 (2020): 69-90.
- Ospina, N y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S1794-1082020000200199&lang=es.
- Pardo, A. (2018). Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/20372/Pardo_VA.pdf?sequence=1&isAllowed=y.
- Peña, O. & Almaza, F. (2010). Teoría Del Delito. <https://derecho.usmp.edu.pe/wpcontent/uploads/2022/05/libro-teoria-del-delito-oscar-pena.pdf>.
- Peña, M. (2022). Delitos Cibernético. <https://repository.unilibre.edu.co/bitstream/handle/10901/24774/TESIS%20VERSION%20APROBADA.pdf?sequence=1&isAllowed=y>
- Rebolledo, R. (2017). El Economista. 14 técnicas para robar tu identidad. <https://www.economista.com.mx/politica/14-tecnicas-para-robar-tu-identidad-20170531-0038.html>.
- Quecedo, R. & Castaño, C. (2002) Introducción a la metodología de investigación cualitativa. <https://www.redalyc.org/pdf/175/17501402.pdf>
- Rizo, J. (2015). Técnicas de investigación Documental. <https://repositorio.unan.edu.ni/12168/1/100795.pdf>.
- Rivera, V. (2019). Realidad sobre los Datos Personales en Costa Rica. https://www.scielo.sa.cr/scielo.php?script=sci_arttext&pid=S1659-41422019002000068&lang=es.
- Rivera, H. (2022). Los delitos informáticos y su incidencia en la gestión de las instituciones del estado del Distrito de Huánuco, 2017. <https://repositorio.unheval.edu.pe/handle/20.500.13080/8160>.
- Sánchez, F. (2019). Fundamentos epistémicos de la investigación cualitativa y cuantitativa: Consensos y disensos. http://www.scielo.org.pe/scielo.php?script=sci_arttext&pid=S2223-25162019000100008#:~:text=Por%20enfoco%20cualitativo%20se%20entiende,Mej%C3%ADa%2C%20como%20se%20cit

%C3%B3%20en

- Sánchez., F. M, & Diaz, J.C. (2021). Técnicas e instrumentos de recolección de información: análisis y procesamiento realizado por el investigador cualitativo. http://scielo.senescyt.gob.ec/scielo.php?script=sci_arttext&pid=S263127862021000300107&lang=es.
- Sarday, Y. (2007). El análisis de información y las investigaciones cuantitativa y cualitativa. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S0864-34662007000300020.
- Solano, D.S., Roldan, M.a. & Vargas, H.F. (2019). Forensic computing methodology in Colombian government institutions: an approach from Law 1952 of 2019. http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S2422-42002023000100122&lang=es.
- Temperini, M. (2018) Delitos informáticos en Latinoamérica: un estudio de derecho comparado. 2da parte. Sociedad Argentina de Informática e Investigación Operativa. <http://sedici.unlp.edu.ar/handle/10915/42145>.
- Tuesta, R. (2022). Fraude informático y su impacto en los derechos fundamentales de la persona en el Cercado de Lima – 2022. https://repositorio.uwiener.edu.pe/bitstream/handle/20.500.13053/8054/T061_46499897_TSP.pdf?sequence=1&isAllowed=y
- Valderrama, A. (2002). Teoría y crítica de la construcción social de la tecnología. file:///H:/fch_editorial,+11278-27286-1-CE.pdf.
- Vences, O.M. (2019). Penalización de los delitos informáticos. (Tesis para optar al título de maestro en derecho-universidad Autónoma del estado de Morelos México). <http://riaa.uaem.mx/xmlui/bitstream/handle/20.500.12055/2675/VESONS06T.pdf?sequence=1&isAllowed=y>
- Vera, V. y Mayer, L.(2022). La falsificación informática: ¿un delito necesario? https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0719-25842022000100261&lang=es
- Vinelli, R. (2021). Los delitos informáticos y su relación con la criminalidad económica. https://revistas.ulima.edu.pe/index.php/Ius_et_Praxis/article/view/4995
- Viorato, R. (2019). La ética en la investigación cualitativa. <http://dx.doi.org/>

10.22201/fesi.23958979e.2019.8.16.70389<https://www.medigraphic.com/pdfs/cuidarte/cui-2019/cui1916e.pdf> .

Zambrano, A. (2020). El uso de banca móvil en los delitos informáticos contra el patrimonio en la ciudad de Arequipa, 2020. [tesis para optar el título profesional de abogado de la Universidad César Vallejo]. <https://repositorio.ucv.edu.pe/handle/20.500.12692/62306>.

Zevallos, V. (2018). Vulneración del Derecho de Propiedad de bienes inmuebles en el Proceso Judicial de Otorgamiento de escritura Pública como consecuencia de un Fraude Procesal. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/31124/Zevallos_VVI.pdf?sequence=1&isAllowed=y

ANEXO 1: Tabla de categorización

Categorías de estudio	Definición conceptual	Categorías	Subcategorías	Código
Fraude informático	Es cuando un individuo a través de las TIC, procura apoderarse de manera ilícita mediante esbozo, entrada, cambio, desvaído, eliminación, duplicación de identificaciones digitales (Artículo 8, Ley 30096).	Fraude informático	Obtención de datos ilegales. Eliminación de datos.	Introducción de datos fraudulentas, estafa virtual, obtención de datos ilegales, eliminación de archivos, clonación de datos.
Vulneración del derecho al patrimonio	Es la violación al derecho irrevocable en la que su extinción y trasmisión obedece al titular la propiedad de los bienes (Zevallos,2018).	Derecho al Patrimonio	Pérdidas materiales. Daños morales.	Vulneración, derecho al patrimonio, daños, pérdidas, materiales, morales.

Nota: Esta tabla muestra las categorías, subcategorías y los códigos del fraude informático y derecho al patrimonio (Fuente Propia).

ANEXO 2: Instrumento de recolección de datos.

GUÍA DE ENTREVISTA

Título: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”

Indicaciones: el presente instrumento pretende recopilar opinión respecto a diferentes temas relacionados a: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”. Por lo cual se pide responder a las siguientes preguntas con neutralidad y precisión, sin necesidad de utilizar citas textuales.

Datos del entrevistado

Apellidos y nombres:

Profesión

Grado académico:

Centro laboral:

Cargo:

Lugar y Fecha: de del 2023

Las preguntas son agrupadas por objetivos, cada una consta de tres preguntas.

Objetivo general

Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023.

Pregunta 1.- según su experiencia ¿Cómo se vulnera el derecho al patrimonio ante un fraude informático? Fundamente su respuesta.

.....
.....
.....

Pregunta 2.- Según su opinión ¿Cuáles son las implicancias y consecuencias del delito del fraude informático? Fundamente su respuesta

.....
.....
.....

Pregunta 3.- Según su experiencia ¿Qué medidas o estrategias de investigación se debe aplicar referente al delito de fraude informático? Fundamente su respuesta.

.....

.....

.....

.....

Objetivo específico 1

Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023

Pregunta 4. Según su experiencia ¿Cómo cree usted que los delincuentes obtienen datos ilegales para ejecutar el delito de fraude informático?

.....

.....

.....

.....

Pregunta 5.- ¿Considera usted que la fiscalía conjuntamente con la alta dirección de tecnología de PNP se encuentra capacitada para afrontar el delito de fraude informático? Fundamente su respuesta.

.....

.....

.....

.....

Pregunta 6.- ¿Considera usted, que el artículo 8 de la Ley 30096 Ley de delitos Informáticos: *“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 3 ni mayor de 8 años**”*; referente a las penas son suficientes para salvaguardar a las personas en la sociedad ante el fraude informático? Fundamente su respuesta.

.....

.....
.....
.....

Objetivo específico 2

Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023

Pregunta 7.- Según su experiencia ¿Considera usted, que ante la comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado pérdida material? Fundamente su respuesta.

.....
.....
.....
.....

Pregunta 8.- Por su experiencia ¿Considera usted, que ante comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado daño moral? Fundamente su respuesta.

.....
.....
.....
.....

Pregunta 9.- Según su experiencia ¿Se compensa completamente el daño moral ocasionado en el delito informático? Fundamente su respuesta.

.....
.....
.....
.....

Finalmente;

10.- ¿Qué opinión le gustaría compartir en relación a la presente investigación?

.....
.....
.....
.....
.....

Nombre del entrevistado	Sello y Firma

ANEXO 3: Consentimiento Informado

CONSENTIMIENTO INFORMADO

Título de la investigación:

“Fraude Informático y El Derecho al Patrimonio en Lima Norte 2023”

Investigador:

Antinógenes Liverato Loarte Poma

Propósito del estudio

Le invitamos a participar en la investigación titulada “Fraude Informático y El Derecho al Patrimonio en Lima Norte 2023”, cuyo objetivo es “Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023”. Esta investigación es desarrollada por el estudiante de pre grado la carrera profesional de DERECHO de la Universidad César Vallejo del campus Lima Norte, aprobado por la autoridad correspondiente de la Universidad y con el permiso de la institución Universidad Cesar Vallejo

Describir el impacto del problema de la investigación.

Al desarrollar el problema de investigación “¿De qué manera el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023?”

Procedimiento

Si usted decide participar en la investigación se realizará lo siguiente

1. Se realizará una entrevista donde se recogerán datos personales y algunas preguntas sobre la investigación titulada: “¿De qué manera el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023?”
2. Esta entrevista tendrá un tiempo aproximado de 5 minutos y se realizará en el ambiente de la Facultad de derecho de la institución Universidad Cesar Vallejo. Las respuestas al guía de entrevista serán codificadas usando un número de identificación y, por lo tanto, serán anónimas.

Puede hacer todas las preguntas para aclarar sus dudas antes de decidir si desea participar o no, y su decisión será respetada. Posterior a la aceptación no desea continuar puede hacerlo sin ningún problema.

Riesgo (principio de No maleficencia):

Indicar al participante la existencia que NO existe riesgo o daño al participar en la investigación. Sin embargo, en el caso que existan preguntas que le puedan generar incomodidad. Usted tiene la libertad de responderlas o no.

Beneficios (principio de beneficencia):

Se le informará que los resultados de la investigación se le alcanzará a la institución al término de la investigación. No recibirá ningún beneficio económico ni de ninguna otra índole. El estudio no va a aportar a la salud individual de la persona, sin embargo, los resultados del estudio podrán convertirse en beneficio de la salud pública.

Confidencialidad (principio de justicia):

Los datos recolectados deben ser anónimos y no tener ninguna forma de identificar al participante. Garantizamos que la información que usted nos brinde es totalmente Confidencial y no será usada para ningún otro propósito fuera de la investigación. Los datos permanecerán bajo custodia del investigador principal y pasado un tiempo determinado serán eliminados convenientemente.

Problemas o preguntas:

Si tiene preguntas sobre la investigación puede contactar con el Investigador LOARTE POMA, ANTINÓGENES LIVERATO email: aloartepo18@ucvvirtual.edu.pe y Docente asesor QUIROZ ROSAS JUAN HUMBERTO, email: jhquirozr@ucvvirtual.edu.pe.

Consentimiento

Después de haber leído los propósitos de la investigación autorizo participar en la investigación antes mencionada.

Nombre y apellidos: Dr. Raymundo Fernando Vargas López, abogado penalista,
Maestro en Derecho Penal y Procesal Penal-Asistente Fiscal – Lima Norte.

Fecha y hora: 6 de octubre del 2023 a las 6:30pm.



Loarte Poma, Antinógenes Liverato
DNI N.º 10403184
Investigador



Raymundo Fernando Vargas López
Reg. CAL N082985
Entrevistado

ANEXO 4: Matriz Evaluación por juicio de expertos, formato UCV.

**ANEXO 3
VALIDACIÓN DE INSTRUMENTO**

I. DATOS GENERALES

a. Apellidos y Nombres : Salas Quispe, Mariano Rodolfo
 b. Cargo e institución donde labora : DTC Universidad Cesar Vallejo
 c. Nombre del instrumento motivo de evaluación: Guía de entrevista
 d. Autor(A) de instrumento : Loarte Poma, Antinógenes diverato
 e. Autor(A) de instrumento : _____

II. ASPECTOS DE VALIDACIÓN


CRITERIOS	INDICADORES	No cumple con su aplicación						Cumple en parte con su aplicación			Si cumple con su aplicación			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible y apropiado.												X	
2. OBJETIVIDAD	Este formulado conforme a los objetivos planteados.												X	
3. ACTUALIDAD	Está formulado, acorde a los aportes recientes del derecho												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 categorías.												X	
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.												X	
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos												X	
9. METODOLOGÍA	Las preguntas obedecen al tipo, diseño y enfoque de la investigación.												X	
10. PERTINENCIA	El instrumento enfrenta un problema crucial jurídico y relevancia global.												X	

III. OPINIÓN DE APLICABILIDAD

El instrumento cumple con los Requisitos para su aplicación	51
El instrumento cumple en parte con los requisitos para su aplicación	
El instrumento no cumple con los requisitos para su aplicación	

IV. PROMEDIO DE VALORACIÓN: 95%

Lima, 20 de junio del 2023.



MARIANO RODOLFO SALAS QUISPE
 ABOGADO
 FIRMA DEL EXPERTO INFORMANTE
 CAL 64800
 DNI N°

DNI N°
ANEXO 3
VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

- a. Apellidos y Nombres : Anaib Huaylupax Juan Carlos
 b. Cargo e institución donde labora : Universidad César Vallejo
 c. Nombre del instrumento motivo de evaluación: Guía de entrevista
 d. Autor(A) de Instrumento : LOARTE POMA, Antinógenes Liverato

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	No cumple con su aplicación						Cumple en parte con su aplicación			Si cumple con su aplicación			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible y apropiado.													X
2. OBJETIVIDAD	Este formulado conforme a los objetivos planteados.													X
3. ACTUALIDAD	Está formulado, acorde a los aportes recientes del derecho													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 categorías.													X
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.													X
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos													X
9. METODOLOGÍA	Las preguntas obedecen al tipo, diseño y enfoque de la investigación.													X
10. PERTINENCIA	El instrumento enfrenta un problema crucial jurídico y relevancia global.													X

III. OPINIÓN DE APLICABILIDAD

El instrumento cumple con los Requisitos para su aplicación	✓
El instrumento cumple en parte con los requisitos para su aplicación	
El instrumento no cumple con los requisitos para su aplicación	

IV. PROMEDIO DE VALORACIÓN:

95%

Lima, 20 de junio del 2023.


 FIRMA DEL EXPERTO INFORMANTE
 DNI N° 09896106

DNI N°
ANEXO 3
VALIDACIÓN DE INSTRUMENTO

I. DATOS GENERALES

- a. Apellidos y Nombres : ROSAS MAYTA KETTY
 b. Cargo e institución donde labora : DTE. UNIVERSIDAD CE MAE VAREJO
 c. Nombre del instrumento motivo de evaluación: Guía de entrevista
 d. Autor(A) de Instrumento : LOARTE POMA, Antinógenes Liverato

II. ASPECTOS DE VALIDACIÓN

CRITERIOS	INDICADORES	No cumple con su aplicación					Cumple en parte con su aplicación			Si cumple con su aplicación				
		40	45	50	55	60	65	70	75	80	85	90	95	100
1. CLARIDAD	Esta formulado con lenguaje comprensible y apropiado.													X
2. OBJETIVIDAD	Este formulado conforme a los objetivos planteados.													X
3. ACTUALIDAD	Está formulado, acorde a los aportes recientes del derecho													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 categorías.													X
7. CONSISTENCIA	Se respalda en fundamentos técnicos y/o científicos.													X
8. COHERENCIA	Existe coherencia entre los problemas, objetivos, supuestos jurídicos													X
9. METODOLOGÍA	Las preguntas obedecen al tipo, diseño y enfoque de la investigación.													X
10. PERTINENCIA	El instrumento enfrenta un problema crucial jurídico y relevancia global.													X

III. OPINIÓN DE APLICABILIDAD

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

IV. PROMEDIO DE VALORACIÓN:

95%

Lima, 20 de junio del 2023.


 FIRMA DEL EXPERTO INFORMANTE
 DNI N° 09794089
 Kelly Rosas Mayra
 ABOGADA
 CAL-45123

ANEXO 6: Escaneo de entrevistas

GUÍA DE ENTREVISTA

Título: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”

Indicaciones: el presente instrumento pretende recopilar opinión respecto a diferentes temas relacionados a: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”. Por lo cual se pide responder a las siguientes preguntas con neutralidad y precisión, sin necesidad de utilizar citas textuales.

Datos del entrevistado

Apellidos y nombres: Augusto Saldaña Alejandro Beder

Profesión: PNP

Grado académico: Superior

Centro laboral: Comisaria Independencia

Cargo: Suboficial Superior PNP

Lugar y Fecha: 25 de setiembre del 2023

Las preguntas son agrupadas por objetivos, cada una consta de tres preguntas.

Objetivo general

Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023.

Pregunta 1.- según su experiencia ¿Cómo se vulnera el derecho al patrimonio ante un fraude informático? Fundamente su respuesta.

Mediante la clonación de tarjetas, sustracción de claves y la vulneración de los aplicativos de los bancos en los celulares, entre otras.

Pregunta 2.- Según su opinión ¿Cuáles son las implicancias y consecuencias del delito del fraude informático? Fundamente su respuesta

El vaciado del dinero de las cuentas bancarias y /o compras por internet.

Pregunta 3.- Según su experiencia ¿Qué medidas o estrategias de investigación se debe aplicar referente al delito de fraude informático? Fundamente su respuesta.

En las operaciones con tarjetas poner un monto mínimo de retiro de transferencias o compras por internet.

Objetivo específico 1

Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023

Pregunta 4. Según su experiencia ¿Cómo cree usted que los delincuentes obtienen datos ilegales para ejecutar el delito de fraude informático?

En los centros nocturnos donde hay ingesta de bebidas alcohólicas, utilizando como dama de compañía a bellas féminas, para que ellas roben sus claves secretas, tejitás de créditos y/o débito, celulares, etc. Mediante la modalidad de pepeo.

Pregunta 5.- ¿Considera usted que la fiscalía conjuntamente con la alta dirección de tecnología de PNP se encuentra capacitada para afrontar el delito de fraude informático? Fundamente su respuesta.

Si, se encuentra capacitado siempre en cuando los agraviados denuncien oportunamente estos hechos.

Pregunta 6.- ¿Considera usted, que el artículo 8 de la Ley 30096 Ley de delitos Informáticos: *“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 3 ni mayor de 8 años”; referente a las penas son suficientes para salvaguardar a las personas en la sociedad ante el fraude informático? Fundamente su respuesta.

Ya que este es el modo operandi de personas de dudosa reputación, que se debe doblar la pena de 12 a 25 años de pena privativa de libertad, sin beneficios carcelarios.

Objetivo específico 2

Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023

Pregunta 7.- Según su experiencia ¿Considera usted, que ante la comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado pérdida material? Fundamente su respuesta.

Si se agravia la totalidad de las cuentas bancarias y / o mercaderías con compras por internet, mediante la usurpación de la propiedad privada.

Pregunta 8.- Por su experiencia ¿Considera usted, que ante comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado daño moral? Fundamente su respuesta.

Si en el fraude informático se ocasiona a el daño moral: porque el que sufre este tipo de robo, tendrán que empezar de nuevo, dejando las cuentas en 0, por esta razón las personas sufren tristeza y depresión.


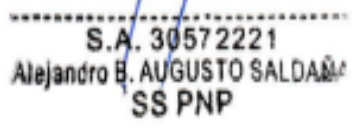
Pregunta 9.- Según su experiencia ¿Se compensa completamente el daño moral ocasionado en el delito informático? Fundamente su respuesta.

Si, se debe compensar el daño moral, siempre en cuando se identifica al culpable, o la persona que perpetró el delito de fraude informático.

Finalmente;

10.- ¿Qué opinión le gustaría compartir en relación a la presente investigación?

En nuestro país las Leyes son muy benignas para cierto tipo de delitos informáticos. Hay personas que les dejan en ruina total y que se debía legislar para que dichas penas sean más drásticas.

Nombre del entrevistado	Sello y Firma
Alejandro Beder Augusto Saldaña	 

GUÍA DE ENTREVISTA

Título: "Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023"

Indicaciones: el presente instrumento pretende recopilar opinión respecto a diferentes temas relacionados a: "Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023". Por lo cual se pide responder a las siguientes preguntas con neutralidad y precisión, sin necesidad de utilizar citas textuales.

Datos del entrevistado

Apellidos y nombres: Mas Guivin Genry

Profesión: Policía

Grado académico: Superior Técnico

Centro laboral: Comisaria Santa Luzmila

Cargo: Suboficial de Segunda

Lugar y Fecha: 29 de setiembre del 2023

Las preguntas son agrupadas por objetivos, cada una consta de tres preguntas.

Objetivo general

Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023.

Pregunta 1.- según su experiencia ¿Cómo se vulnera el derecho al patrimonio ante un fraude informático? Fundamente su respuesta.

Las denuncias por el delito Contra el Patrimonio – Fraude Informático, con el pasar de los años se han venido incrementando de manera alarmante toda vez que a través de la tecnología los delincuentes de dotan de diversas herramientas para cometer los delitos

especialmente a través de las redes, lo que hace más compleja la investigación para la Policía Nacional del Perú.

Pregunta 2.- Según su opinión ¿Cuáles son las implicancias y consecuencias del delito del fraude informático? Fundamente su respuesta

En la actualidad todos los ciudadanos nos encontramos expuestos a ser víctima de este tipo de delitos, lo que genera inseguridad y falta de confianza al momento de confiar su dinero o sus ahorros en una entidad bancaria ya que están expuestos a que los delincuentes puedan clonar sus tarjetas o emplear hackers para vulnerar sus cuentas bancarias.

Pregunta 3.- Según su experiencia ¿Qué medidas o estrategias de investigación se debe aplicar referente al delito de fraude informático? Fundamente su respuesta.

La policía nacional del Perú, al tomar conocimiento sobre un hecho ilícito en la modalidad de Fraude Informático, procede a poner de conocimiento de ministerio público, la noticia criminal a fin de que de manera coordinada pueda agotar los medios y emplear herramientas para la identificación y la posible detención del presunto autor o autores del hecho ilícito siempre y cuando se encuentre en flagrante delito; asimismo, se exhorta a los ciudadanos tener cuidado al momento de hacer uso de sus tarjetas bancarias y cuando hace retiro de dinero en las agencias y/o cajeros automáticos.

Objetivo específico 1

Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023

Pregunta 4. Según su experiencia ¿Cómo cree usted que los delincuentes obtienen datos ilegales para ejecutar el delito de fraude informático?

Generalmente los delincuentes usan nuestra propia información lo cual obtienen a través de llamadas telefónicas, mensajes de texto o mensajes de WhatsApp donde se hacen pasar por asesores bancarios ofreciendo prestamos o facilidades para obtener tarjetas bancarias para lo cual solicitan brinden información estrictamente confidencial como numero de tarjetas y clave secreta.

Pregunta 5.- ¿Considera usted que la fiscalía conjuntamente con la alta dirección de tecnología de PNP se encuentra capacitada para afrontar el delito de fraude informático? Fundamente su respuesta.

Teniendo en cuenta que la modalidad del delito de fraude informativo es un tipo penal nuevo, tanto el ministerio público, así como la policía nacional vienen realizando denodados esfuerzos con la finalidad de combatir ese tipo de ilícitos; sin embargo, no es suficiente el esfuerzo o empeño que acarrea realizar dicha investigación ya que se necesita de medios tecnológicos y herramientas sofisticadas para detectar e identificar a los presuntos responsables de los delitos ya mencionados.

Pregunta 6.- ¿Considera usted, que el artículo 8 de la Ley 30096 Ley de delitos Informáticos: *“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 3 ni mayor de 8 años”*; referente a las penas son suficientes para salvaguardar a las personas en la sociedad ante el fraude informático? Fundamente su respuesta.

Las penas estipuladas en la presente ley no son suficientes ante la perpetración de dicho delito ya que teniendo la opción entre 3 y 8 años, corre la posibilidad que dicha pena sea suspendida de libertad y que el autor sea citado y investigado en su domicilio, de donde puede seguir delinquiendo ya que no necesita transitar o desplazarse por las calles para cometer el ilícito y lo puede realizar a través de la tecnología, empleando una computadora, laptop, aparatos móviles o cualquier aparato electrónico que le puede ser útil.

Objetivo específico 2

Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023

Pregunta 7.- Según su experiencia ¿Considera usted, que ante la comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado pérdida material? Fundamente su respuesta.

Definitivamente se vulnera el derecho al patrimonio, ya que en muchos casos este tipo de delitos queda impune debido a que no se logra dar con el paradero o identificar al autor o autores del hecho ilícito, mas aun si es que el usuario no paga un seguro contra robo en la entidad bancaria es casi imposible que pueda recuperar su dinero.

Pregunta 8.- Por su experiencia ¿Considera usted, que ante comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado daño moral?

Fundamente su respuesta.

Definitivamente afecta el daño moral ya que al momento que ser afectado el bien patrimonial el agraviado entra en un estado depresivo y de incertidumbre al no saber como se pudo generar dicha acción.

Pregunta 9.- Según su experiencia ¿Se compensa completamente el daño moral ocasionado en el delito informático? Fundamente su respuesta.

Al ser víctima del delito contra el patrimonio – Fraude Informático, la persona agraviada ya no vuelve a recuperar la confianza ya que la afectación emocional es evidente y así recupere su patrimonio siempre queda una inseguridad al momento de realizar algún trámite o transacción bancaria.

Finalmente;

10.- ¿Qué opinión le gustaría compartir en relación a la presente investigación?

Es necesario realizar modificatorias en la norma que sanciona el Fraude Informático, toda vez que en muchos casos el delito cometido no reúne todos los presupuestos establecidos para que el autor pueda ser sancionado con una pena privativa de libertad. Asimismo, el gobierno debe dotar de material logístico y tecnología sofisticada para la investigación de este tipo de hechos.

Nombre del entrevistado	Sello y Firma
GENRY MAS GUIVIN	 CIP. 31616182 GENRY MAS GUIVIN S2 - PNP

GUÍA DE ENTREVISTA

Título: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”

Indicaciones: el presente instrumento pretende recopilar opinión respecto a diferentes temas relacionados a: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”. Por lo cual se pide responder a las siguientes preguntas con neutralidad y precisión, sin necesidad de utilizar citas textuales.

Datos del entrevistado

Apellidos y nombres: Asca Robles Alejandro

Profesión: Abogado

Grado académico: Superior

Centro laboral: Estudio Jurídico Independiente

Cargo: abogado penalista

Lugar y Fecha: 26 de setiembre del 2023

Las preguntas son agrupadas por objetivos, cada una consta de tres preguntas.

Objetivo General

Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023.

Pregunta 1.- según su experiencia ¿Cómo se vulnera el derecho al patrimonio ante un fraude informático? Fundamente su respuesta.

Se vulnera mediante la, eliminación, supresión, modificación, de datos de los sistemas informáticos en sus distintas modalidades según la Ley N° 30096 que lo contempla.

Pregunta 2.- Según su opinión ¿Cuáles son las implicancias y consecuencias del delito del fraude informático? Fundamente su respuesta

Referente a las implicancias y consecuencias del delito de fraude informático, éstas se realizan investigaciones en la DIVINDAT y Fiscalía Especializada de la Ciberdelincuencia.

Pregunta 3.- Según su experiencia ¿Qué medidas o estrategias de investigación

se debe aplicar referente al delito de fraude informático? Fundamente su respuesta.

- Denuncias oportunas a la policía o fiscalías de delitos informáticos.
- Pericias informáticas, para determinar el sistema usado.
- Información a entidades bancarias en caso de fraude informático.

Objetivo específico 1

Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023

Pregunta 4. Según su experiencia ¿Cómo cree usted que los delincuentes obtienen datos ilegales para ejecutar el delito de fraude informático?

- Mediante la suplantación de identidad.
- Valiéndose de llamadas y/o mensajes simuladas.
- Clonación de tarjetas robadas.

Pregunta 5.- ¿Considera usted que la fiscalía conjuntamente con la alta dirección de tecnología de PNP se encuentra capacitada para afrontar el delito de fraude informático? Fundamente su respuesta.

Si, ya que existen unidades especializadas como son la DIVINDAT y la fiscalía de la ciberdelincuencia, que están trabajando referente a delitos informáticos en caso de fraude informático.

Pregunta 6.- ¿Considera usted, que el artículo 8 de la Ley 30096 Ley de delitos Informáticos: “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 3 ni mayor de 8 años”; referente a las penas son suficientes para salvaguardar a las personas en la sociedad ante el fraude informático? Fundamente su respuesta.

Si, en base al principio de proporcionalidad en sentido estricto y las penas deben ser mayores desde 8 años a 20 años de pena privativa de libertad.

Objetivo específico 2

Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023

Pregunta 7.- Según su experiencia ¿Considera usted, que ante la comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado pérdida material? Fundamente su respuesta.

Si se vulnera el derecho al patrimonio cuando se roba el secreto de los datos propios del patrimonio protegido por la ley y los derechos fundamentales.

Pregunta 8.- Por su experiencia ¿Considera usted, que ante comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado daño moral? Fundamente su respuesta.

Sufren trastornos emocionales. desespero, angustia, inseguridad económica y perturbaciones fisiológicos en general.

Pregunta 9.- Según su experiencia ¿Se compensa completamente el daño moral ocasionado en el delito informático? Fundamente su respuesta.


No, se puede compensar el daño moral, debido a que, en el delito de fraude informático, no se puede identificar a los autores, dado la modalidad delictiva empleada, ya muchas veces se cometen desde lugares alejados, otros países. Departamentos alejados, hasta de la prisión.

Finalmente;

10.- ¿Qué opinión le gustaría compartir en relación a la presente investigación?

Dotar de mayor capacitación del personal del DIVINDAT - PNP, Jueces, fiscales y operadores jurídicos y mayor presupuesto para equipamiento con alta tecnología para

la identificación, detección, juzgamiento y sanción de autores del delito de fraude informático.

Nombre del entrevistado	Sello y Firma
Dr. Alejandro Asca Robles	

GUÍA DE ENTREVISTA

Título: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”

Indicaciones: el presente instrumento pretende recopilar opinión respecto a diferentes temas relacionados a: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”. Por lo cual se pide responder a las siguientes preguntas con neutralidad y precisión, sin necesidad de utilizar citas textuales.

Datos del entrevistado

Apellidos y nombres: Saravia Gonzales Poldark

Profesión: Abogado

Grado académico: Maestro

Centro: Docente

Lugar y Fecha: 04 de octubre del 2023

Las preguntas son agrupadas por objetivos, cada una consta de tres preguntas.

Objetivo general

Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023.

Pregunta 1.- según su experiencia ¿Cómo se vulnera el derecho al patrimonio ante un fraude informático? Fundamente su respuesta.

Debemos entender que el derecho al patrimonio es un derecho inescrutable. Pero ante los actos dolosos configurados en el tipo penal fraude informático, la integridad de un patrimonio se ve trasgredido, mancillado y quebrantado.

Pregunta 2.- Según su opinión ¿Cuáles son las implicancias y consecuencias del delito del fraude informático? Fundamente su respuesta

Las influencias y/o consecuencias son:

- i) Robo de información personal.
- ii) Reducción de patrimonio.

Todo ello en perjuicio de los afectados.

Pregunta 3.- Según su experiencia ¿Qué medidas o estrategias de investigación se debe aplicar referente al delito de fraude informático? Fundamente su respuesta.

Las medidas a tomar son:

- i) Protección de nuestra información.
- ii) Tener claves o contraseñas seguros.
- iii) No proporcionar los datos sin considerar la seguridad del receptor.

Objetivo específico 1

Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023

Pregunta 4. Según su experiencia ¿Cómo cree usted que los delincuentes obtienen datos ilegales para ejecutar el delito de fraude informático?

Hoy en día acceder a la base de datos informacional de las personas naturales y/o jurídicas es muy sencillo de adherirse, existen lugares donde por un robo te obtienen esta información. Ejemplo centro comercial de Wilson.

Pregunta 5.- ¿Considera usted que la fiscalía conjuntamente con la alta dirección de tecnología de PNP se encuentra capacitada para afrontar el delito de fraude informático? Fundamente su respuesta.

Considero que sí, aunque, con el avance vertiginoso de la informática, las fiscalías especializadas en delitos cibernéticos, y la DIVINDAT de la PNP deben capacitarse constantemente.

Pregunta 6.- ¿Considera usted, que el artículo 8 de la Ley 30096 Ley de delitos Informáticos: “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 3 ni mayor de 8 años”; referente a las penas son suficientes para salvaguardar a las personas en la sociedad ante el fraude informático? Fundamente su respuesta.

Considero que las penas privativas de libertad deben estar en proporción a la infracción cometida por el sujeto activo. En ese sentido deben aumentar la pena.

Objetivo específico 2

Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023

Pregunta 7.- Según su experiencia ¿Considera usted, que ante la comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado pérdida material? Fundamente su respuesta.

Si, debido a que es una disminución de patrimonio, por lo que le genera pérdidas al sujeto afectado por el fraude informático.

Pregunta 8.- Por su experiencia ¿Considera usted, que ante comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado daño moral? Fundamente su respuesta.

Se debe entender por daño moral a la afectación de una acción que causa angustia o sufrimiento. El cual debe resarcirse. En ese sentido el ser afectado emocionalmente, debe conllevar a una compensación económica por parte del sujeto activo.


Pregunta 9.- Según su experiencia ¿Se compensa completamente el daño moral ocasionado en el delito informático? Fundamente su respuesta.

No, debido a que no se puede medir el daño moral en ese sentido los delitos informáticos se ajustan a sus efectos.

Finalmente;

10.- ¿Qué opinión le gustaría compartir en relación a la presente investigación?

Considero que la investigación, aporta nuevas nociones e ideas que las autoridades competentes deben considerar al tratar este delito y por otro lado los sujetos afectados deben tomar las precauciones y/o contingencias al respecto.

Nombre del entrevistado	Sello y Firma
Mg. Poldark Saravia Gonzales DNI: 41388688	 Poldark Saravia Gonzales ABOGADO C.A.L. N° 51530

GUÍA DE ENTREVISTA

Título: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”

Indicaciones: el presente instrumento pretende recopilar opinión respecto a diferentes temas relacionados a: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”. Por lo cual se pide responder a las siguientes preguntas con neutralidad y precisión, sin necesidad de utilizar citas textuales.

Datos del entrevistado

Apellidos y nombres: Benites García José Ismael

Profesión: Abogado

Grado académico: Magister

Centro laboral: Universidad Cesar Vallejo

Cargo: Docente SUBE-UCV

Lugar y Fecha: 29 de setiembre del 2023

Las preguntas son agrupadas por objetivos, cada una consta de tres preguntas.

Objetivo General

Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023.

Pregunta 1.- según su experiencia ¿Cómo se vulnera el derecho al patrimonio ante un fraude informático? Fundamente su respuesta.

Se vulnera realizando conductas previstas en la Ley de Delitos Informáticos N° 30096 y sus modificatorias.

Pregunta 2.- Según su opinión ¿Cuáles son las implicancias y consecuencias del delito del fraude informático? Fundamente su respuesta

La implicancia mediante la afectación patrimonial y afectación moral de las personas naturales y/o jurídicas. Consecuencias Fomenta la inseguridad ciudadana.

Pregunta 3.- Según su experiencia ¿Qué medidas o estrategias de investigación se debe aplicar referente al delito de fraude informático? Fundamente su respuesta.

Especialización en materia de ciberdelincuencia nivel de fiscalías, jueces, operadores de justicia y la División de Investigación de Delitos de Alta Tecnología de la PNP (DIVINDAT-PNP).

Objetivo específico 1

Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023

Pregunta 4. Según su experiencia ¿Cómo cree usted que los delincuentes obtienen datos ilegales para ejecutar el delito de fraude informático?

A través de ataques cibernéticos por los hackers, la vulneración de los archivos en el sistema financiero y el quebrantamiento de datos personales o claves secretas de las personas naturales y/lo jurídicas.

Pregunta 5.- ¿Considera usted que la fiscalía conjuntamente con la alta dirección de tecnología de PNP se encuentra capacitada para afrontar el delito de fraude informático? Fundamente su respuesta.

En la actualidad falta mayor capacitación y dotación de herramientas tecnológicas para combatir el delito de fraude informático.

Pregunta 6.- ¿Considera usted, que el artículo 8 de la Ley 30096 Ley de delitos Informáticos: *“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 3 ni mayor de 8*

años”; referente a las penas son suficientes para salvaguardar a las personas en la sociedad ante el fraude informático? Fundamente su respuesta.

Un mayor incremento de la pena no garantiza para memorar el delito; se debe atacar en forma integral, mediante políticas de prevención, información adecuada a la ciudadanía, equipamiento y capacitación al DIVINDAT de la PNP, a los fiscales, jueces y operadores de justicia.

Objetivo específico 2

Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023

Pregunta 7.- Según su experiencia ¿Considera usted, que ante la comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado pérdida material? Fundamente su respuesta.

La comisión de fraude informático si, afecta primordialmente al patrimonio neto de las personas naturales y/o jurídicas.

Pregunta 8.- Por su experiencia ¿Considera usted, que ante comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado daño moral? Fundamente su respuesta.

La comisión de fraude informático, si vulnera teniendo como resultado el daño moral, que consiste en la preocupación, ansiedad, desorden fisiológico, como dolor de estómago, náuseas, palpitaciones, irritabilidad, entre muchas según la salud física y la edad.

Pregunta 9.- Según su experiencia ¿Se compensa completamente el daño moral ocasionado en el delito informático? Fundamente su respuesta.


Muchas veces no se compensa el daño moral ocasionado en el delito informático, ya que no se puede acreditar el hecho afectado moralmente.

Finalmente;

10.- ¿Qué opinión le gustaría compartir en relación a la presente investigación?

Que se analice y tenga en cuenta la Ley de Delitos Informáticos Ley N° 30096 y su modificatoria Ley N° 30171. Y la observancia de casos fiscales sobre ciberdelincuencia que está a disposición y de acceso del público.

Recomendamos denunciar hechos de robo de celulares, tarjetas de créditos, débitos y a las llamas anónimas amenazadoras al celular N° 942 440 729 o al correo electrónico divindat.servicioguardia@policia.gob.pe .

Nombre del entrevistado	Sello y Firma
Dr. Benites García José Ismael	 ----- ICAP 2082 Docente SUBE - UCV Docente de la Facultad de Derecho y Humanidades - UCV Especialidad: Derecho Penal-Aula 823 B

GUÍA DE ENTREVISTA

Título: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”

Indicaciones: el presente instrumento pretende recopilar opinión respecto a diferentes temas relacionados a: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”. Por lo cual se pide responder a las siguientes preguntas con neutralidad y precisión, sin necesidad de utilizar citas textuales.

Datos del entrevistado

Apellidos y nombres: Jiménez Rufino, Violeta

Profesión: Abogado

Grado académico: Magister

Centro laboral: Docente_ Universidad Cesar Vallejo

Cargo: Docente SUBE-UCV

Lugar y Fecha: 14 de octubre del 2023

Las preguntas son agrupadas por objetivos, cada una consta de tres preguntas.

Objetivo General

Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023.

Pregunta 1.- según su experiencia ¿Cómo se vulnera el derecho al patrimonio ante un fraude informático? Fundamente su respuesta.

El derecho al patrimonio es un derecho inalienable, exclusivo, propia, sin embargo, ante los actos dolosos configurados en el tipo penal fraude informático, la integridad de un patrimonio se ve quebrantado, deshonrado y mancillado.

Pregunta 2.- Según su opinión ¿Cuáles son las implicancias y consecuencias del delito del fraude informático? Fundamente su respuesta

Las influencias y/o consecuencias son: a) Sustracción de información propia, b) Disminución de heredad o patrimonio. Todo ello en perjuicio de los afectados mediante el fraude informático.

Pregunta 3.- Según su experiencia ¿Qué medidas o estrategias de investigación se debe aplicar referente al delito de fraude informático? Fundamente su respuesta.

Especialización referente al fraude informático nivel de fiscalías, jueces, operadores de justicia y la División de Investigación de Delitos de Alta Tecnología de la PNP (DIVINDAT-PNP). Y la información a la ciudadanía sobre la protección de sus datos de manera segura, no exponer informaciones privadas a personas desconocidas o en redes sociales.

Objetivo específico 1

Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023

Pregunta 4. Según su experiencia ¿Cómo cree usted que los delincuentes obtienen datos ilegales para ejecutar el delito de fraude informático?

Utilizando especialistas en cibernética, ingresando a base de datos como los hackers, la vulneración de los archivos en el sistema financiero y comercial, mediante el quebrantamiento de datos personales o claves secretas de las personas naturales y/o jurídicas.

Pregunta 5.- ¿Considera usted que la fiscalía conjuntamente con la alta dirección de tecnología de PNP se encuentra capacitada para afrontar el delito de fraude informático? Fundamente su respuesta.

Considero que sí, aunque, con el avance acelerado del tratamiento de la información, las fiscalías especializadas en delitos cibernéticos, y la DIVINDAT de la PNP deben capacitarse constantemente.

6.- ¿Considera usted, que el artículo 8 de la Ley 30096 Ley de delitos Informáticos: “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 3 ni mayor de 8 años”; referente a las penas son suficientes para salvaguardar a las personas en la sociedad ante el fraude informático? Fundamente su respuesta.

Las penas privativas de libertad deben estar en proporción a la infracción cometida por el sujeto activo. En ese sentido deben aumentar la pena, de 5 a 10 años. Para que la pena sea efectiva.

Objetivo específico 2

Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023

Pregunta 7.- Según su experiencia ¿Considera usted, que ante la comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado pérdida material? Fundamente su respuesta.

Si, afecta la comisión de fraude informático al vulnerar el derecho al patrimonio, mediante la pérdida del patrimonio del sujeto perjudicado por el fraude informático.

Pregunta 8.- Por su experiencia ¿Considera usted, que ante comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado daño moral? Fundamente su respuesta.

Entendido el daño moral a la acción que causa pena, angustia o sufrimiento. El cual debe repararse. El ser afectado emocionalmente, debe ser sujeto a una compensación económica por parte del sujeto activo.

Pregunta 9.- Según su experiencia ¿Se compensa completamente el daño moral ocasionado en el delito informático? Fundamente su respuesta.


No se compensa el daño moral ocasionado en el delito informático, ya que no se puede acreditar el hecho afectado moralmente que se ajusten a sus efectos.

Finalmente;

10.- ¿Qué opinión le gustaría compartir en relación a la presente investigación?

Que el trabajo de investigación es pertinente ya que trata de delitos que se cometen frecuentemente en la actualidad. Recomendamos denunciar hechos de robo de celulares, tarjetas de créditos, débitos y a las llamas anónimas amenazadoras al

celular N° 942 440 729 o al correo electrónico divindat.servicioguardia@policia.gob.pe .

Sello y Firma	
Nombre del entrevistado	
Mg., Violeta Jiménez Rufino	Violeta Jiménez Rufino DNI 03647818
	Especialista en Derecho Pena – Catedrática de la Facultad de Derecho y Humanidades - UCV Especialidad: Derecho Penal – Pabellón A - Aula 806A

GUÍA DE ENTREVISTA

Título: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”

Indicaciones: el presente instrumento pretende recopilar opinión respecto a diferentes temas relacionados a: “Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023”. Por lo cual se pide responder a las siguientes preguntas con neutralidad y precisión, sin necesidad de utilizar citas textuales.

Datos del entrevistado:

Apellidos y nombres: Martínez Castro Juan Carlos

Profesión: Abogado

Grado académico: Magister

Centro laboral: Ministerio Publico _ Universidad Cesar Vallejo

Cargo: Fiscal – Docente SUBE-UCV

Lugar y Fecha: 23 de setiembre del 2023

Las preguntas son agrupadas por objetivos, cada una consta de tres preguntas.

Objetivo General

Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023.

Pregunta 1.- según su experiencia ¿Cómo se vulnera el derecho al patrimonio ante un fraude informático? Fundamente su respuesta.

Se vulnera mediante la alteración, supresión de sistemas informáticos en sus distintas modalidades de la Ley N° 30096 y sus modificatorias.

Pregunta 2.- Según su opinión ¿Cuáles son las implicancias y consecuencias del delito del fraude informático? Fundamente su respuesta

Dentro de las implicancias y consecuencias esta que se realizan investigaciones en la DIVINDAT y Fiscalía Especializada de la Ciberdelincuencia.

Pregunta 3.- Según su experiencia ¿Qué medidas o estrategias de investigación se debe aplicar referente al delito de fraude informático? Fundamente su respuesta.

- Reportar la pérdida o robo de las tarjetas y/o dispositivo móvil a entidades correspondientes para el bloqueo de las claves de los chips.
- Denuncias oportunas a la policía o fiscalías de delitos informáticos.
- Pericias informáticas, para determinar el sistema usado.
- Información a entidades bancarias en caso de fraude informático.

Objetivo específico 1

Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023

Pregunta 4. Según su experiencia ¿Cómo cree usted que los delincuentes obtienen datos ilegales para ejecutar el delito de fraude informático?

- Mediante la suplantación de identidad.
- Valiéndose de llamadas simuladas.
- Simulando ofertas y/o regalos de una entidad benéfica.

Pregunta 5.- ¿Considera usted que la fiscalía conjuntamente con la alta dirección de tecnología de PNP se encuentra capacitada para afrontar el delito de fraude informático? Fundamente su respuesta.

Si, ya que existen unidades especializadas como son la DIVINDAT y la fiscalía de la ciberdelincuencia.

Pregunta 6.- ¿Considera usted, que el artículo 8 de la Ley 30096 Ley de delitos Informáticos: *“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 3 ni mayor de 8 años”*; referente a las penas son suficientes para salvaguardar a las personas en la sociedad ante el fraude informático? Fundamente su respuesta.

Si, en base al principio de proporcionalidad en donde media la idoneidad y la proporcionalidad en sentido estricto.

Objetivo específico 2

Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023

Pregunta 7.- Según su experiencia ¿Considera usted, que ante la comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado pérdida material? Fundamente su respuesta.

Si se vulnera el derecho al patrimonio; pero no se vulnera el derecho a la información mediante los delitos informáticos.

Pregunta 8.- Por su experiencia ¿Considera usted, que ante comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado daño moral? Fundamente su respuesta.

Sí, pero muchas veces en caso de delitos fraude informático se ve la imposibilidad de obtener y recuperar su patrimonio causando daño psicológico.

Pregunta 9.- Según su experiencia ¿Se compensa completamente el daño moral ocasionado en el delito informático? Fundamente su respuesta.

No, se puede compensar completamente el daño moral, debido a que, en muchos casos en el delito de fraude informático, no se puede identificar a los autores, dado la modalidad delictiva empleada.

Finalmente;

10.- ¿Qué opinión le gustaría compartir en relación a la presente investigación?

Que en la actualidad la DIVINDAT-DIRINCRI, se encuentran saturadas en las pericias informáticas que se suelen requerir de los medios y dispositivos usados: Por otra parte, en trabajo de investigación es muy actualizada y pertinente.

Nombre del entrevistado	Sello y Firma
Dr. Juan Carlos Martínez Castro	 <p>Fiscal Adjunto Lima Norte Ministerio Público y Docente - UCV</p>  <p>MINISTERIO PÚBLICO FISCALÍA DE LA NACIÓN Distrito Fiscal de Lima Norte</p>

GUÍA DE ENTREVISTA

Título: "Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023"

Indicaciones: el presente instrumento pretende recopilar opinión respecto a diferentes temas relacionados a: "Fraude Informático y el Derecho al Patrimonio en Lima Norte 2023". Por lo cual se pide responder a las siguientes preguntas con neutralidad y precisión, sin necesidad de utilizar citas textuales.

Datos del entrevistado

Apellidos y nombres: Vargas López Raymond Fernando

Profesión: Abogado

Grado académico: Maestro en Derecho Penal y Procesal Penal / Maestro en Gestión Pública.

Centro laboral: Ministerio Público

Cargo: Asistente en Función Fiscal

Lugar y Fecha: 06 de octubre del 2023

Las preguntas son agrupadas por objetivos, cada una consta de tres preguntas.

Objetivo general

Determinar la manera que el delito del fraude informático vulnera al derecho del patrimonio en Lima Norte 2023.

Pregunta 1 según su experiencia ¿Cómo se vulnera el derecho al patrimonio ante un fraude informático? Fundamente su respuesta.

La finalidad de cometer el delito de fraude informático es obtener un beneficio económico, por ejemplo, transfiriendo dinero de una persona a la cuenta del delincuente, con lo cual causa un perjuicio a la víctima, porque le están robando prácticamente su dinero, pero de manera virtual utilizando medios electrónicos.

Pregunta 2.- Según su opinión ¿Cuáles son las implicancias y consecuencias del delito del fraude informático? Fundamente su respuesta

La consecuencia de la comisión de este delito para la víctima es que va perder su patrimonio monetario principalmente, lo cual le va causar gran afectación para su vida por otro lado, si el delincuente que cometió el delito es capturado será investigado y

podrá ser reprimido con una pena privativa de la libertad no menor de 03 años, ni mayor de 8 años, y con 60 a 120 días multa.

Pregunta 3.- Según su experiencia ¿Qué medidas o estrategias de investigación se debe aplicar referente al delito de fraude informático? Fundamente su respuesta.

Estos delitos deben ser investigados por servidores y funcionarios públicos debidamente capacitados y que cuenten con las herramientas tecnológicas para poder realizar de manera correcta una investigación, siendo que es necesario que la Unidad Fiscal Especializada en Ciberdelincuencia lleve estos casos.

Objetivo específico 1

Determinar la manera que se accede a nuestra información privada para cometer el delito de fraude informático en Lima Norte 2023

Pregunta 4. Según su experiencia ¿Cómo cree usted que los delincuentes obtienen datos ilegales para ejecutar el delito de fraude informático?

Los delincuentes que cometen estos delitos son personas expertas en tecnologías de la información, siendo que tienen amplio conocimiento del manejo de redes y dispositivos informáticos, por lo que pueden obtener información hackeando cuentas de WhatsApp, Facebook o Instagram, además también se cometen estos delitos cuando se roba o hurta un teléfono celular.

Pregunta 5.- ¿Considera usted que la fiscalía conjuntamente con la alta dirección de tecnología de PNP se encuentra capacitada para afrontar el delito de fraude informático? Fundamente su respuesta.

Considero que la Unidad Fiscal Especializada en Ciberdelincuencia de Lima cuenta con un laboratorio tecnológico, personal de apoyo (ingenieros de sistemas), servidores y funcionarios públicos debidamente capacitados para poder realizar una correcta investigación sobre el delito de fraude informático y sobre otros delitos informáticos.

Pregunta 6.- ¿Considera usted, que el artículo 8 de la Ley 30096 Ley de delitos Informáticos: "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 3 ni mayor de 8 años"; referente a las penas son suficientes para salvaguardar a las personas en la sociedad ante el fraude informático? Fundamente su respuesta.

Considero que la pena debe aumentar, debería ser una pena no menor de 04 ni mayor de 08 años, para que la pena que se dicte sea efectiva y no suspendida.

Objetivo específico 2

Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración a nuestro patrimonio en Lima Norte 2023

Pregunta 7.- Según su experiencia ¿Considera usted, que ante la comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado pérdida material? Fundamente su respuesta.

Considero que sí, porque se puede transferir dinero a la cuenta del delincuente, afectando el patrimonio de la víctima.

Pregunta 8.- Por su experiencia ¿Considera usted, que ante comisión del fraude informático se vulnera el derecho al patrimonio teniendo como resultado daño moral? Fundamente su respuesta.

Considero que sí, porque al perder su patrimonio monetario, las victimas pueden deprimirse por ver frustrados sus proyectos que tenían planeados.

Pregunta 9.- Según su experiencia ¿Se compensa completamente el daño moral ocasionado en el delito informático? Fundamente su respuesta.

Considero que no, porque las victimas generalmente quedan afectadas moralmente por haber sufrido esta situación,

Finalmente

10.- ¿Qué opinión le gustaría compartir en relación a la presente investigación?

Considero que el tema de tesis es interesante e importante.

Nombre del entrevistado	Sello y Firma
Raymond Fernando Vargas López	 <p>Raymond Fernando Vargas López Abogado Reg. CAL N°82985 Asistente en Función Fiscal- Lima Norte</p>  <p>MINISTERIO PÚBLICO FISCALÍA DE LA NACIÓN Distrito Fiscal de Lima Norte</p>