Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

LA REGULACIÓN JURÍDICA DE DELITOS INFORMATICOS CONTRA EL PATRIMONIO EN LA LEGISLACIÓN PENAL, EN LA CORTE SUPERIOR DE LIMA NORTE 2023

Línea de investigación:
Procesos jurídicos y resolución de conflictos

Tesis para optar el grado académico de Maestro en Derecho Penal

Autor

Caro Guzmán, Jonathan Martín

Asesor

Laos Jaramillo, Enrique Jordán

ORCID: 0000-0002-2061-1293

Jurado

Jiménez Herrera, Juan Carlos

Ambrosio Bejarano, Hugo Ramiro

Panduro Angulo, Eckerman

Lima - Perú

2026

LA REGULACIÓN JURÍDICA DE DELITOS INFORMATICOS CONTRA EL PATRIMONIO EN LA LEGISLACIÓN PENAL, EN LA CORTE SUPERIOR DE LIMA NORTE 2023

INFORME DE ORIGINALIDAD

27%	27%	2%	14%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	16%
2	revistas.pj.gob.pe Fuente de Internet	3%
3	repositorio.upsc.edu.pe Fuente de Internet	2%
4	repositorio.ucv.edu.pe Fuente de Internet	2%
5	Submitted to Universidad Cesar Vallejo Trabajo del estudiante	1%
6	Submitted to Universidad Nacional Federico Villarreal Trabajo del estudiante	<1%
7	www.slideshare.net Fuente de Internet	<1%
8	repositorio.unfv.edu.pe Fuente de Internet	<1%

Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

ESCUELA UNIVERSITARIA DE POSGRADO

LA REGULACIÓN JURÍDICA DE DELITOS INFORMÁTICOS CONTRA EL PATRIMONIO EN LA LEGISLACIÓN PENAL, EN LA CORTE SUPERIOR DE LIMA NORTE 2023

Línea de investigación:

Procesos Jurídicos y Resolución de Conflictos

Tesis para optar el grado académico de

Maestro en Derecho Penal

Autor

Caro Guzmán, Jonathan Martín

Asesor

Laos Jaramillo, Enrique Jordán

ORCID: 0000-0002-2061-1293

Jurado

Jiménez Herrera, Juan Carlos

Ambrosio Bejarano, Hugo Ramiro

Panduro Angulo, Eckerman

Lima – Perú

2026

ÍNDICE

INDICE DE TABLAS

INDICE DE FIGURAS

RESUMEN

El presente trabajo de investigación titulado “La regulación jurídica de delitos informáticos contra el patrimonio en la legislación penal, en la corte superior de lima norte 2023”. En cuanto al enfoque metodológico, nuestra investigación adopta un enfoque cuantitativo básico, es un método de investigación que utiliza herramientas de análisis matemático y estadístico para describir, explicar y predecir fenómenos mediante datos numéricos, además prueba la hipótesis y la teoría. Por último, mide los fenómenos. Para el análisis de datos, se emplean métodos analíticos, deductivos, lo que permite que puedan ser aplicados a otros ámbitos, en concordancia con los procedimientos de muestreo y las limitaciones prestablecidas. La técnica de recolección de datos utilizada fue la encuesta, con una escala de 14 preguntas aplicada, a 278 expertos en delitos informáticos, qué son la muestra, de la población de 1000.Profesionales expertos en Derecho Penal. Lo cual se obtuvo información precisa para realizar nuestro cuadro estadístico. Soy Abogado en función, tengo ya 10 años en el campo de la litigación Oral, lo que más se ha visto, el incremento de estos delitos informáticos, es con el ingreso de los delincuentes venezolanos a nuestro país, en el 2018, los delitos informáticos se han incrementado de 5% a un 70%. imagínese todos estamos expuestos al hakeo y de ser robados nuestros datos informáticos, con el desarrollo de las TIC, ha surgido un nuevo tipo de delito asociado al uso de computadoras, motores de búsqueda, sistemas telemáticos y la gestión de información, que afecta cuentas comerciales, financieras y personales. En América Latina se están implementando varias medidas al respecto. En nuestro país, se aprobó el convenio sobre ciberdelincuencia mediante la Resolución Legislativa N° 30913 el 12 de febrero de 2019, y fue ratificado por el Ejecutivo con el Decreto Supremo N° 010-2019-RE el 10 de marzo de 2019.

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

ABSTRACT

This research paper, entitled "The Legal Regulation of Cybercrimes against Property in Criminal Law, Lima North Superior Court 2023," is presented here. Regarding the methodological approach, our research adopts a basic quantitative approach. This research method uses mathematical and statistical analysis tools to describe, explain, and predict phenomena through numerical data. It also tests hypotheses and theories and ultimately measures the phenomena. For data analysis, analytical and deductive methods are employed, allowing them to be applied to other fields, in accordance with the sampling procedures and pre-established limitations. The data collection technique used was the survey, with a scale of 14 questions applied, to 278 experts in computer crimes, who are the sample, of the population of 1000. Professionals' expert in Criminal Law. I am a practicing lawyer with ten years of experience in oral litigation. The most noticeable increase in cybercrimes has been the influx of Venezuelan criminals into our country. In 2018, cybercrimes increased from 5% to 70%. Imagine, we are all exposed to hacking and having our computer data stolen. With the development of ICTs, a new type of crime has emerged associated with the use of computers, search engines, telematics systems, and information management, affecting commercial, financial, and personal accounts. Several measures are being implemented in Latin America to address this. In our country, the convention on cybercrime was approved by Legislative Resolution No. 30913 on February 12, 2019, and was 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

1.1. Planteamiento del problema

El avance tecnológico ha impulsado un notable incremento en las comunicaciones, lo que, a su vez, ha facilitado el surgimiento y evolución de delitos, mediante la manipulación de sistemas informáticos. Esto incluye la alteración, daño o eliminación de archivos y datos digitales, acciones que pueden llevarse a cabo desde cualquier ubicación con acceso a internet.

Desde finales del siglo XX, se dio un impulso significativo en las ciencias aplicadas a la mecanización y las tecnologías de la información. El hardware se volvió más compacto y versátil, mientras que el software se hizo más ágil y fácil de usar. Con la creación de los teléfonos celulares con conectividad a la web y la capacidad de conectarse con otros dispositivos, así como la interconexión de los sistemas informáticos en entidades financieras, compañías privadas y organizaciones de servicios, y el aumento masivo del uso de ordenadores, se facilitó el crecimiento de delitos cibernéticos, siendo uno de los más comunes el fraude informático.

Debido al incremento de actividades fraudulentas en línea, los gobiernos están implementando una variedad de estrategias para resguardar la información de los usuarios almacenada en la web. Asimismo, la evolución tecnológica ha fomentado el crecimiento del trabajo remoto y del comercio en línea, lo que a su vez ha facilitado la expansión de estafas en el entorno digital, infracciones que transgreden las leyes de tutela al usuario. Los países del orbe enfrentan una enorme tarea en cuanto a la normativización de políticas de ciberseguridad y la normativa sobre IA.

1.2. Descripción del problema

En los últimos años, al analizar comparativamente las leyes sobre delitos informáticos en América Latina, se ha observado que varios países, como República Dominicana, Puerto Rico y Costa Rica, han promulgado legislaciones específicas para proteger los datos personales,

especialmente en casos de robo de identidad digital. En Costa Rica, por ejemplo, la protección de la identidad personal es considerada un derecho fundamental, con los ciudadanos teniendo el control constitucional sobre sus datos y la gestión de su información privada, amparados por la constitución de ese país (Rivera, 2019).

En Perú, los ciberdelitos representan un peligro significativo para la economía, la democracia, las libertades individuales, y los recursos y servicios esenciales. Durante el año 2022, se registró el robo de aproximadamente 8500 millones de datos personales, que fueron vendidos y explotados tras ser obtenidos mediante ataques cibernéticos. Los delincuentes en el ámbito digital siguen adaptándose rápidamente a los cambios sociales, económicos y tecnológicos (Ospina, 2020).

Durante el 2021, en Perú, se registraron 5,620 denuncias relacionadas con delitos informáticos, mientras que, en 2022, la Dirección de Investigación Criminal de Alta Tecnología (DIVIDANT) de la Policía Nacional del Perú revisó 3,946 denuncias de este tipo. En esos años, las autoridades lograron capturar a 135 individuos en 2021 y a 229 en 2022. Esto equivale a un 2.4% y un 5.8% de detenciones respectivamente, lo que evidencia un bajo índice de capturas en comparación con la cantidad de delitos reportados. Esta información fue divulgada en un medio oficial (El Peruano, 17 septiembre 2023).

En ausencia de una investigación sobre este problema, se anticipan consecuencias altamente negativas. La proliferación de fraudes en línea ha llevado a un aumento en los delitos cibernéticos, impulsado por el uso generalizado de plataformas digitales. Si se incorporan modalidades de delitos como "Phishing, Vishing, Smishing, Carding y Pharming" a la Ley de Delitos Informáticos, la interacción entre el delincuente y la víctima se reduce al mínimo. Esto se debe a que la recolección de datos bancarios se realiza de manera casi imperceptible a través de técnicas como el redireccionamiento de páginas web, permitiendo su uso ilegal sin la necesidad del engaño explícito que actualmente exige nuestro Código Penal (Fuente,2021).

Partimos de la premisa de que, si no se incorporan los tipos penales como phishing, vishing, smishing, carding y pharming en el Código Penal y, al mismo tiempo, no se fortalecen las estrategias y mecanismos de tutela contra los delitos informáticos, la ciberdelincuencia seguirá poniendo en riesgo el patrimonio tanto individual como nacional.

Nuestro método de investigación es de tipo cuantitativo y posee una significancia científica. Específicamente, empleamos técnicas dirigidas a la recolección detallada de información, como la realización de encuestas y el uso de estas encuentas nos permitirá obtener datos. A través de estos procedimientos, obtenemos datos sobre hechos relevantes y temas de estudio, con el objetivo de analizar principales incidentes delictivos y sus repercusiones desde una perspectiva legal, tales como la pérdida de bienes a través de engaños, robos y fraudes en línea (Sánchez, 2021).

1.3. Formulación del problema

1.3.1. Problema general

¿De qué manera se da los delitos informáticos contra el patrimonio en la legislación penal, en la corte superior de lima norte 2023”

1.3.2. Problemas específicos

¿De qué manera se accede a nuestra información privada para cometer el delito de fraude informático, en la corte superior de lima norte 2023”

¿Cuáles son los daños materiales y morales que ocasionan el fraude informático con la vulneración, en la corte superior de lima norte 2023”

1.4. Antecedentes

El engaño digital y la infracción del derecho a la propiedad fueron vistos como temas innovadores y actuales en las investigaciones realizadas en plataformas en línea con recursos científicos y diferentes fuentes, como Cybertesis, EBSCO, el repositorio de la universidad y SCIELO, etc. Además, la proliferación de teléfonos móviles, tabletas, computadoras portátiles

y de escritorio, todos conectados a Internet, ha dado lugar a nuevos fenómenos delictivos vinculados al crimen informático.

Los antecedentes de esta investigación se basaron en el estudio de artículos de revistas, reportes científicos y textos, utilizando plataformas en línea que indexan tesis tanto a nivel nacional como internacional.

Respecto a los antecedentes internacionales, en Colombia, una investigación de maestría defendida por Peña (2023) en el área de delitos cibernéticos señala que el uso creciente de internet está llevando a un aumento en los ataques cibernéticos dirigidos a instituciones financieras, bancarias y comerciales, lo cual está impactando a la población y representando un desafío significativo para el Estado.

Sichaca (2019) En su trabajo académico, el autor concluye que la normativa actual sobre pruebas digitales es insuficiente. Señala la necesidad de una comprensión profunda de los principios legales y procesales, así como de los métodos y procedimientos para presentar pruebas digitales de manera válida. En resumen, los profesionales del derecho deben estar bien informados y actualizados sobre los avances tecnológicos en el ámbito de los delitos digitales, ya que la legislación exige estar al día para enfrentar eficazmente estas actividades.

Rincón (2015) en su tesis doctoral, argumenta que las fronteras nacionales no deberían impedir la investigación y el enjuiciamiento efectivo de los delitos cibernéticos. Destaca que, en el ciberespacio, sin límites físicos, la ubicación del delincuente puede ser distinta a la de la víctima, lo que hace esencial definir la jurisdicción para sancionar. El autor aboga por la creación de un sistema de justicia universal, enfocándose en el Derecho Comparado y la Cooperación Internacional.

Duarte (2017) en su obra investiga cómo los documentos audiovisuales se relacionan con las pruebas ilegales y las protecciones constitucionales relacionadas con su obtención. También evalúa la importancia probatoria y la aceptabilidad de estos documentos en el

contexto del proceso penal.

Además, en México, Vences (2019) presentó una tesis que argumenta que el derecho informático se está estableciendo como una disciplina jurídica novedosa. Esto se debe a que el crecimiento de la información a través de dispositivos conectados a internet demanda nuevos mecanismos normativos para asegurar la tutela de los datos que estos dispositivos almacenan.

En cuanto a los antecedentes nacionales en Perú, Tuesta (2022), en su tesis para obtener el título de abogado, afirma que el fraude informático ha aumentado considerablemente en los últimos años, impactando negativamente los derechos fundamentales de las personas en Lima. Este aumento se debe en parte a la complejidad de identificar a los responsables.

Escobedo (2018) afirma que los crímenes cibernéticos están intrínsecamente ligados a Internet, dando lugar a infracciones transnacionales que superan las limitaciones de leyes y jurisdicciones nacionales. Estos delitos pueden involucrar a varios países en un solo incidente. Dado que tales delitos se cometen en el entorno digital, es fundamental contar con herramientas tecnológicas para llevar a cabo estas acciones. En particular, Internet actúa como el canal a través del cual se transmiten los datos necesarios para ejecutar estos actos ilícitos, permitiendo que la violación de derechos ocurra sin importar las fronteras geográficas, desde distancias cortas hasta largas y, a veces, atravesando continentes. Esto plantea el desafío de definir el alcance territorial y establecer el marco legal adecuado para abordar y sancionar estos delitos.

Abanto (2016), en su tesis, examina detalladamente la falta de protección adecuada de los datos personales, explorando las diversas formas en que ocurre esta exposición y cómo se aplican los métodos de prueba en el ámbito penal. El autor subraya la urgencia de una legislación específica que se adapte a la evolución de las pruebas digitales, destacando la importancia de que estas pruebas sean confiables y legales para que puedan ser utilizadas efectivamente en los procesos judiciales. En consecuencia, proporciona un análisis completo de las técnicas apropiadas para la búsqueda y recolección de pruebas digitales, al tiempo que

propone políticas e iniciativas a nivel nacional y global en ciberseguridad.

En su tesis doctoral, Chávez (2018) sostiene que los crímenes dirigidos contra los secretos digitales impactan los derechos fundamentales individuales.

De manera similar, Goñi (2021), en su trabajo de tesis para conseguir el título de abogado en Perú, señala que el aumento en el uso del Internet ha dado paso a una nueva era de delitos cibernéticos.

De igual manera, en la Universidad Nacional Federico Villareal, la tesis de Blossiers (2018) sostiene que no se ha establecido un adecuado marco legal para los delitos informáticos, lo que significa que el actual sistema no garantiza de manera adecuada la protección de los derechos de personas, empresas y organizaciones.

De igual modo, Rivera (2022) señala en su tesis doctoral que las acciones delictivas cibernéticas, llevadas a cabo particularmente por funcionarios, perjudican tanto a las entidades privadas como a las públicas de manera adversa.

En su tesis, Ancco (2021) argumenta que existe una conexión directa entre el crimen organizado y la ejecución de actividades delictivas, y propone que el Poder Judicial refuerce la formación de quienes intervienen en el sistema.

1.5. Justificación de la investigación

La justificación teórica de este estudio se basa en el hecho de que, durante la pandemia de COVID-19, se observó un aumento en el teletrabajo y en las transacciones crediticias analógicas. Este crecimiento facilitó un incremento en los ataques a los archivos de los usuarios bancarios en línea, llevados a cabo a través de engaños para robar dinero depositado. Según datos de la Policía Nacional del Perú (PNP) y del Observatorio Nacional de Política Criminal (ONPC), las denuncias de ciberdelitos crecieron significativamente entre 2020 y 2021, pasando de un 25% a un 65% (Chero, 2022). En cuanto a la justificación práctica, esta investigación busca ofrecer perspectivas para mejorar el sistema jurídico informático. Desde el punto de vista

metodológico, se empleará información sobre jurisprudencias, aspectos legales y entrevistas con expertos en el tema, aplicando el método científico.

1.6. Limitaciones de la investigación

En cuanto a las limitaciones, en primera instancia se hizo un poco complicado la búsqueda de información de este tipo penal dentro del ámbito peruano debido a que, se advirtió que el desarrollo tanto normativo como doctrinal está más avanzando en otras naciones en comparación con el nuestro. Al margen de ello, la investigación no ha presentado mayores limitaciones.

1.7. Objetivos

1.7.1. Objetivo general

Determinar de qué manera:

"el delito del fraude informático vulnera contra el patrimonio en la legislación penal, en la corte superior de lima norte 2023"

1.7.2. Objetivos específicos

Determinar la manera que se accede a nuestra información privada:

"Identificar los daños materiales y morales que ocasionan el fraude informático con la vulneración, en la corte superior de lima norte 2023"

Figura 1

Manipulación informática privada.

Tabla 1

Número de denuncias por delitos informáticos registrados en la PNP según departamento, 2019-202

CUADRO 01 » Número de denuncias por delitos informáticos registrados en la PNP según departamento, 2019-2021

Lima	4,139	4,527	7,324
Arequipa	496	645	877
La Libertad	483	602	835
Callao	341	510	774
Lambayeque	306	466	719
Piura	223	325	576
Tacna	83	126	426
Ancash	193	285	405
Huánuco	80	232	358
Junín	58	162	338
Cusco	178	225	308
Ica	115	142	236
San Martín	31	73	189
Ucayali	47	85	187
Moquegua	56	83	184
Loreto	78	92	167
Puno	19	49	163
Ayacucho	36	42	142
Cajamarca	26	57	120
Amazonas	45	49	101
Apurímac	21	46	66
Pasco	9	34	62
Huancavelica	20	15	51
Tumbes	16	18	34
Madre de Dios	9	7	29
Total	7,108	8,897	14,671
Variación porcentual		25%	65%

Fuente: PNP, SIDPOL, información preliminar
Elaboración: Observatorio Nacional de Política Criminal INDAGA

II. MARCO TEÓRICO

2.1. Marco conceptual

Crimen digital: Un crimen digital abarca cualquier acción ilícita ejecutada en el entorno virtual o mediante el uso de tecnología informática y de comunicación. Estas acciones abarcan estafas en internet, intrusiones informáticas, sustracción de información, propagación de software dañino y otras conductas perjudiciales con intenciones ilegales.

Legislación Digital: La legislación digital comprende el sistema normativo que regula todo lo relacionado con las acciones en la red y las conductas en el ámbito virtual. Esta normativa aborda específicamente los delitos cibernéticos, fija sanciones por infracciones y establece las bases legales para la investigación y persecución de delitos relacionados con la tecnología.

Evidencia Digital: La evidencia digital abarca toda información o datos en formato electrónico que se pueden usar en un juicio para corroborar afirmaciones o cargos. Esto engloba desde historiales de navegación y correos electrónicos hasta mensajes y archivos, sirviendo para probar la ocurrencia de delitos cibernéticos o para identificar a los responsables.

La ingeniería social: Se refiere a la práctica de influir en el comportamiento de las personas para que lleven a cabo acciones específicas o compartan información privada. En el ámbito de los delitos cibernéticos, esto puede involucrar la manipulación de individuos para que entreguen contraseñas, detalles financieros u otros datos sensibles, con la intención de ejecutar fraudes en internet o realizar otros ataques.

Delincuente cibernético: es una persona o un grupo que se dedica a realizar actividades ilícitas en la red. Estos individuos emplean sus conocimientos técnicos para cometer crímenes en línea, como el phishing, el robo de identidades, la propagación de software malicioso o el hackeo de sistemas, con el objetivo de obtener ganancias económicas o provocar daño.

2.2. Teorías

Para explorar en detalle la categoría del fraude informático, Mayer y Olivera (2020) discuten en su artículo publicado en una revista indexada chilena que el término "delito informático" hace referencia a una actividad que integra las características fundamentales de un delito. Esta actividad implica la utilización indebida de componentes informáticos, violando los derechos de los propietarios de los equipos, dispositivos físicos, o sistemas lógicos.

El peruano Espinoza (2022) argumenta que los reportes sobre fraudes cibernéticos llevados a cabo a través de internet representan un riesgo constante para la ciudadanía, además de presentar un desafío considerable para las autoridades policiales debido a la complejidad y especialización que caracteriza este tipo de delitos. La falta de denuncias y reportes complica aún más la identificación de los delincuentes responsables, tanto para la PNP como para los fiscales. En relación con el fraude informático, el Artículo 8 de la Ley 30096 establece que cualquier uso ilegal de las TIC, como el diseño, ingreso, modificación, eliminación, interrupción o duplicación de datos informáticos con fines de lucro, será penado con una condena de entre 3 y 8 años de prisión y una multa de 70 a 120 días.

En el mismo artículo, se establece un agravante que implica una pena de prisión de entre 5 y 10 años, junto con una multa de 80 a 140 días, para quienes violen o alteren bienes del Estado destinados al apoyo de los más necesitados. Asimismo, en el Convenio sobre la Ciberdelincuencia, que entró en vigor en diciembre de 2019, el artículo 8 señala que los países signatarios deben promover leyes que prevengan, intervengan y castiguen a quienes cometen delitos en línea, especialmente aquellos perpetrados por personas que operan desde distintos países.

De acuerdo con Jiménez (2017), el fraude informático se caracteriza por ser una práctica ilícita que persigue la ganancia personal mediante la manipulación, borrado, destrucción o pérdida de información en dispositivos electrónicos. Asimismo, Vinelli (2021)

indica que el período entre 2020 y 2021 experimentó un notable incremento en el comercio en línea, impulsado por el auge de los pagos y compras digitales, lo cual ha traído consigo importantes avances, pero también ha facilitado la proliferación de actividades criminales en internet, destacando el fraude informático entre ellas.

Este fenómeno ha transformado significativamente el panorama de la seguridad digital, creando un entorno más vulnerable a ataques cibernéticos. La expansión del comercio electrónico y la adopción generalizada de plataformas digitales han abierto nuevas avenidas para el fraude informático, permitiendo a los delincuentes explotar debilidades en los sistemas de pago y en la protección de datos personales. Con el crecimiento exponencial de las transacciones en línea, la sofisticación de las técnicas de fraude también ha evolucionado, exigiendo una mayor capacidad de respuesta por parte de las instituciones financieras y los usuarios para protegerse contra estos riesgos emergentes. La creciente interconexión global y la dependencia de las tecnologías digitales hacen imperativo el desarrollo de estrategias de seguridad más robustas para mitigar estos delitos y proteger tanto a consumidores como a empresas.

Arias (2021) señala que en el campo de la informática emergen varios elementos criminológicos relevantes: en primer lugar, el "conocimiento" vinculado al avance y perfeccionamiento de los sistemas informáticos representa un riesgo, ya que estos sistemas ahora gestionan enormes cantidades de datos diversos. En segundo lugar, el peligro se hace evidente cuando la información es mal utilizada, lo que genera peligros en una comunidad que se caracteriza por su alta competitividad. La tecnología de la información no solo incrementa el poder de quienes la controlan, sino que también exacerba las desigualdades y plantea desafíos a los derechos y garantías fundamentales dentro de un estado democrático. Por último, el mal uso de la informática a menudo resulta en daños graves para las víctimas.

Además, este panorama de riesgo destaca la necesidad urgente de implementar medidas

de seguridad más rigurosas y efectivas. La creciente sofisticación de las herramientas informáticas amplifica la capacidad de los delincuentes para cometer fraudes y otras actividades ilícitas, exponiendo a individuos y organizaciones a riesgos significativos. La extensión de la técnica de los datos y su integración en todas las dimensiones de la cotidianidad de la vida y empresarial han transformado el entorno en el que operan los delincuentes, facilitando la ejecución de delitos con mayor eficacia y menor riesgo de detección. En consecuencia, es crucial desarrollar y aplicar estrategias de protección robustas, que incluyan educación continua sobre ciberseguridad, innovaciones en tecnología de protección y una regulación más estricta para salvaguardar la integridad de los sistemas informáticos y los derechos de las personas en un marco digital cada vez más complejo y vulnerable.

El Tratado de Budapest es el único instrumento internacional que aborda particularmente la problemática de los delitos cibernéticos, concentrándose en las infracciones cometidas a través de la tecnología y en el entorno digital. Este acuerdo internacional se dedica a la identificación y el combate de los cibercriminales, fomentando la cooperación internacional al armonizar las legislaciones sobre delitos informáticos y regulando el ámbito digital. El primer acuerdo global de este tipo fue suscrito en Budapest el 23 de noviembre de 2001, y su implementación comenzó en Europa el 1 de julio de 2004. En el caso de Perú, la adhesión a este tratado se oficializó a través de la Resolución Legislativa N° 30913 el 12 de febrero de 2019, y fue ratificada por el Ejecutivo mediante el Decreto Supremo N° 010-2019-RE el 10 de marzo de 2019.

Uno de los principales argumentos a favor del término "cibercrimen" es que este concepto se ajusta más adecuadamente a las conductas delictivas que se llevan a cabo mediante internet y redes electrónicas similares. Dado que el internet ha posibilitado la creación del ciberespacio, los delitos que ocurren "dentro de" o "a través de" este entorno deberían ser clasificados como cibercrímenes en lugar de delitos informáticos (Borbúa et al., 2017).

Castillo (2020) señala que uno de los motivos clave para optar por el término "cibercrimen" en lugar de "delito informático" es que el primero abarca una gama más amplia de delitos que tienen en común el uso de medios electrónicos o el ciberespacio para su comisión. Según Miró (2012), delitos como el acoso sexual en línea, el hostigamiento de menores a través de la red o smartphones, y la incitación al terrorismo en entornos virtuales encajan mejor con la noción de "cibernético" que con la de "informático". Así, el término "cibercrimen" se emplea para describir cualquier conducta delictiva que utilice elementos cibernéticos (Acurio, 2017). Para esta perspectiva, cualquier delito que involucre tecnología informática o telemática en su ejecución o resultado debe ser considerado un cibercrimen.

Dado que las tecnologías de comunicación y el internet facilitan una amplia gama de actividades delictivas posibles a través de estos medios, se prefiere utilizar los términos "cibercrimen" o "ciberdelito" en lugar de "delito informático", que es más limitado y sujeto a interpretaciones jurídicas variadas que no capturan toda la complejidad de la criminalidad asociada con los sistemas informáticos y telemáticos.

El enfoque conceptual de esta indagación se basa en la descripción de Abushihab (2017), quien define el fraude informático como un comportamiento que pone en riesgo bienes tutelados por la ley de individuos o entidades. Este tipo de delito técnico-criminal se caracteriza por el acceso, modificación, ocultación o eliminación no autorizada de datos en un sistema informático, así como la distribución o venta no consentida de estos datos.

La globalización ha impulsado el avance tecnológico al facilitar la creación de herramientas digitales, revolucionando cómo se realizan diversas actividades. Este fenómeno ha optimizado la comunicación y acelerado los procesos, pero también ha incrementado los riesgos de violación de los bienes jurídicos en el ámbito digital. Así, mientras la tecnología ha ofrecido grandes beneficios, también ha dado lugar a nuevas formas de criminalidad (Chavarría, 2023).

Cada año, nuestras autoridades, tanto locales como nacionales, se esfuerzan intensamente para combatir los delitos en el ciberespacio. No obstante, los logros hasta ahora han sido insatisfactorios, ya que estos delitos continúan en ascenso. Esta situación se debe a múltiples causas: leyes inadecuadas, insuficiente capacitación de los profesionales del ámbito judicial, y falta de recursos logísticos y tecnológicos necesarios para una persecución efectiva de estos crímenes, entre otros.

El prematuro progreso de las tecnologías de la información y la comunicación (TIC) presenta un reto para el marco legal, dado que induce cambios profundos en el derecho penal y la estrategia contra el crimen. A medida que la tecnología progresa, también lo hace la delincuencia, desplazándose cada vez más al ámbito digital. Por lo tanto, la digitalización exige la creación de un sistema legal y políticas criminales que se adapten eficazmente a las nuevas circunstancias emergentes en el mundo digital (Espinoza Prado, 2022).

Villavicencio (2014) sostiene que, aunque la tecnología ofrece numerosas ventajas en distintos contextos, también conlleva un aumento en los riesgos delictivos vinculados al uso de sistemas informáticos y medios de comunicación. Por tanto, el progreso tecnológico no solo ha hecho más ágiles las interacciones, sino que ha dado lugar a nuevas modalidades de crimen, empleando los sistemas informáticos e internet como herramientas.

No estamos hablando de una simple delincuencia ordinaria, sino de una criminalidad profundamente arraigada y sofisticada, con consecuencias más graves. Las víctimas pueden ser desde individuos vulnerables como ancianos, niños o personas con escaso conocimiento informático, hasta individuos con alta capacidad económica. En esencia, nadie está protegido de esta modalidad de crimen tecnológico.

Por ello, la ciberdelincuencia representa un nuevo reto para nuestro sistema legal, así como también para aquellas instituciones que se encargan de hacer cumplir la norma, incluyendo a la policía, la fiscalía y la autoridad judicial, pues estas entidades a menudo se ven

superadas por los ciberdelincuentes que, en su mayoría, poseen conocimientos especializados en informática, mientras que los profesionales de nuestro sistema legal carecen de formación en esta área (Espinoza Calderón, 2022)

Por ello, resulta crucial asignar valores a los nuevos bienes jurídicos y crear leyes para su protección, de modo que se subsanen los vacíos legales existentes. Estos temas deben ser prioritarios para los legisladores, ya que, de no hacerlo, la impunidad seguirá siendo alta. La aparición del internet ha multiplicado las oportunidades para cometer delitos en lugares previamente inimaginables (Espinoza Prado, 2022). Este fenómeno continúa creciendo y evolucionando, planteando un desafío importante para las fuerzas policiales y las autoridades judiciales en su lucha contra esta forma de criminalidad.

No cabe duda de que los crímenes en el ámbito digital han aumentado de manera alarmante y superado las limitaciones tecnológicas. Los delincuentes se valen del avance digital y de las herramientas disponibles para llevar a cabo ataques extremadamente elaborados contra sus víctimas, lo cual provoca serias repercusiones económicas (Anicama, 2023). Esta situación plantea un verdadero reto tanto para la seguridad en línea como para la estabilidad económica global, por lo que el sistema legal debe estar preparado para enfrentar esta forma de delito.

Según Barrio (2017), los ciberdelitos son violaciones legales que ocurren en el ciberespacio, un ámbito artificial generado por los medios informáticos. Esta categoría no se limita a los delitos que afectan a los equipos, datos o sistemas informáticos (que comprometen la integridad, confidencialidad y disponibilidad), sino que también incluye los delitos convencionales perpetrados a través de dispositivos electrónicos o digitales, tales como amenazas, coacciones y estafas. En esencia, los ciberdelitos abarcan una amplia gama de actividades delictivas que suceden en el entorno virtual y que implican tanto aspectos informáticos como comportamientos tradicionales realizados mediante tecnologías digitales.

Tobares y Castro (2010) presentan una definición que refleja una idea similar a la

anterior. Afirman que el delito informático abarca cualquier violación legal en la que se utilicen computadoras o tecnologías relacionadas. Este tipo de crimen ocurre cuando la computadora se emplea como herramienta o como objetivo en la actividad delictiva. Según estos autores, el delito informático incluye cualquier conducta ilegal que implique el uso de tecnología electrónica, ya sea como método, medio o meta de la acción criminal (p. 28). En términos más estrictos, se clasifica como tipo penal informático cualquier acto delictivo donde los ordenadores, sus técnicas y funciones desempeñan un rol clave, ya sea como método, medio o fin del crimen. Es importante recordar que estos delitos están profundamente vinculados con la aplicación de la tecnología informática en diversas formas y contextos delictivos.

De acuerdo con Flores (2014), los delitos informáticos se definen como cualquier conducta, ya sea una acción o una omisión, que está estipulada y castigada por la ley, y que es realizada por alguien en el ámbito de la informática. Esta conducta tiene como resultado el daño a individuos concretos y la obtención de beneficios ilícitos por parte del perpetrador. Flores también identifica varios aspectos esenciales para reconocer estos delitos, que son los siguientes:

i. El bien jurídico tutelado es la integridad y seguridad de los sistemas informáticos implicados.
ii. El elemento subjetivo se refiere a la intención (dolo) o negligencia (culpa) del autor del delito.
iii. El autor de estos delitos generalmente posee un grado de conocimiento y educación, como programadores, analistas de sistemas, expertos en comunicaciones, supervisores, y personal técnico y de mantenimiento.
iv. Las víctimas más comunes suelen ser las entidades bancarias, que realizan transacciones mediante símbolos electrónicos (p. 132).

El autor menciona que los delitos informáticos a menudo se cometen durante las

actividades laborales, dado que los delincuentes digitales suelen aprovechar su entorno de trabajo para llevar a cabo estos actos delictivos. Esto se debe a que las oportunidades para cometer estos delitos surgen en el contexto laboral, donde los ciberdelincuentes pueden sacar ventaja de situaciones propicias. Además, estos delitos ocasionan pérdidas económicas significativas para las víctimas, mientras que los delincuentes obtienen beneficios que a veces superan los cinco dígitos. Estas acciones también se ejecutan con facilidad en cuanto a tiempo y espacio, ya que pueden realizarse rápidamente sin necesidad de la presencia física de los autores.

También se indica que, pese a la frecuente ocurrencia de estos crímenes, una gran cantidad no recibe castigo por las complicaciones en su comprobación, derivadas de su carácter técnico. La mayoría de ellos son intencionales y deliberados. La alarmante escalada de estos delitos resalta la necesidad urgente de establecer normativas tanto nacionales como internacionales para abordar efectivamente este problema en expansión.

Desde la visión de Segrera y Cano (2010), una de las principales dificultades del sistema judicial para enfrentar los delitos informáticos radica en la carencia de formación especializada entre los profesionales del derecho. No todos poseen un conocimiento profundo en este campo, lo que plantea un reto considerable para asegurar la presencia de expertos legalmente capacitados en esta área particular (p. 221).

Uno de los pilares esenciales en la gestión, ya sea en el sector público o privado, es la idea de que la información es clave para el poder. En la actualidad, la administración eficiente de la información es vital para dirigir organizaciones que enfrentan cambios continuos. Para los gestores en el ámbito de la justicia penal, las nuevas tecnologías de la información y comunicación ofrecen oportunidades para optimizar el control operativo, la toma de decisiones y la planificación estratégica, elementos cruciales para el éxito de las instituciones judiciales, como la policía, los tribunales y los centros correccionales.

En el pasado, los problemas de delincuencia informática se resolvían principalmente mediante el uso de programas y controles tecnológicos, bajo la idea de que la solución estaba en la tecnología misma. Sin embargo, con la llegada de nuevos sistemas de prevención, los ciberdelincuentes han desarrollado nuevas formas de sortear estas medidas. Por ello, los expertos en el ámbito penal, conscientes de la complejidad de los delitos tecnológicos, deben contar con conocimientos específicos para llevar a cabo investigaciones y juicios eficaces en este campo. A pesar del aumento en la incidencia de crímenes informáticos, sigue habiendo una notable falta de profesionales de la justicia con el conocimiento necesario para identificar, investigar y enjuiciar estos delitos (Segrera y Cano, 2010).

Así, la intrincada y cambiante naturaleza de los delitos informáticos resalta la urgencia de contar con profesionales especializados, cuyas competencias se basen en una constante actualización en tecnologías digitales. En contraste, la falta de estas habilidades fundamentales para investigar crímenes en el ámbito informático dificulta su correcta persecución. En consecuencia, una formación inadecuada puede provocar que los jueces ignoren o interpreten erróneamente pruebas clave en casos relacionados con sistemas informáticos.

Es crucial proporcionar una formación rápida y efectiva a los profesionales del derecho en este campo, ya que jueces, fiscales, policías y abogados deben tener un conocimiento sólido para lidiar con estos delitos. Sin una preparación adecuada, podríamos enfrentar serios problemas en la investigación. Por lo tanto, es fundamental que la capacitación en derecho informático sea una prioridad desde la educación universitaria. La inclusión obligatoria de este curso en los programas académicos es esencial para cubrir temas clave como comercio electrónico, firma digital, documentos electrónicos, delitos informáticos, pruebas digitales y otros aspectos relevantes (Espinoza Calderón, 2022).

De manera similar, la capacitación sobre delitos cibernéticos no debe ser exclusiva de las fiscalías especializadas; debe abarcar todas las fiscalías, comisarías, tribunales y demás

organismos pertinentes, dado que estos delitos pueden surgir en cualquier rincón del país. Por ende, es crucial ofrecer formación a la ciudadanía y llevar a cabo campañas informativas y preventivas a través de charlas en escuelas, asociaciones, medios de comunicación y otros canales. En resumen, se debe promover una cultura digital que impulse el uso adecuado y responsable de internet en toda la sociedad.

Según Tejada (2017), para abordar los delitos de manera efectiva, es esencial disponer de marcos legales que faciliten la investigación criminal y optimizar el uso de la tecnología en la lucha contra la criminalidad (p. 34). Además, es importante destacar que diariamente enfrentamos diversos problemas, siendo uno de los más destacados la lentitud en la obtención de datos de los proveedores de servicios de internet. Esto se debe a que estos proveedores aún no cuentan con mecanismos en línea para tramitar solicitudes de conservación de datos u otros procedimientos, y también existe una resistencia continua por parte de estos proveedores para revelar información sobre sus usuarios.

Cada dispositivo conectado a Internet posee una etiqueta digital exclusiva llamada dirección IP. No obstante, hay múltiples métodos para ocultar esta etiqueta o hacer parecer que la conexión proviene de otro lugar, lo cual enmascara la identidad del delincuente cibernético. Esto complica enormemente el trabajo de las autoridades encargadas de rastrear y combatir delitos en el entorno digital.

Desde la visión de Barrio (2017), la batalla contra la ciberdelincuencia enfrenta múltiples dificultades debido a diversos factores técnicos que complican la identificación y el enjuiciamiento de los delitos en línea, lo que agrava el problema de la ciberdelincuencia. En este contexto, el anonimato se presenta como un factor clave (p. 43), ya que ofrece a los delincuentes cibernéticos una capa protectora que dificulta su identificación, complicando así el trabajo de las autoridades para rastrear y llevar ante la justicia a quienes cometen delitos en el ciberespacio.

En esta perspectiva, el autor identifica dos aspectos fundamentales que complican o hacen inviable la lucha contra el crimen cibernético. El primero es el anonimato del delincuente, y el segundo, la ejecución remota del delito. En cuanto al anonimato, es relevante destacar que, frecuentemente, es difícil determinar la identidad del perpetrador en delitos cometidos a través de plataformas digitales. Así, identificar plenamente al autor detrás de un ciberdelito puede resultar un desafío considerable.

Para abordar esto, es crucial entender que cada aparato que se conecta a la red presenta una dirección IP, que actúa como una especie de "identificación digital" del dispositivo. Aunque detectar y rastrear esta dirección IP podría parecer sencillo al principio, dado que es un dato público y personal, existen métodos para ocultarla o modificarla. Estos métodos incluyen el uso de redes wifi-abiertas, proxies, redes privadas virtuales (VPN) y la formación de redes botnet (Barrio, 2017).

El principal obstáculo para los fiscales y las fuerzas del orden en las investigaciones penales es la invisibilidad de los ciberdelincuentes. Por ejemplo, en situaciones de fraude en línea, aunque se logre descubrir quién es el propietario de la cuenta que recibió los fondos transferidos sin autorización desde la cuenta de la víctima, no siempre se puede atribuir la responsabilidad a esa persona, ya que quien recibe el dinero no siempre es el que realizó las transacciones fraudulentas (Espinoza Calderón, 2022).

Se presentan numerosos casos en los que las cuentas que reciben transferencias fraudulentas a menudo pertenecen a otras víctimas. A veces, los criminales se apoderan de múltiples cuentas y las emplean para fines ilícitos, usándolas como receptores. Para llevar a cabo estos actos delictivos, los ciberdelincuentes engañan a las víctimas, logrando que estas les den, de manera culpable, toda la información requerida para robarles su dinero.

Los delincuentes cibernéticos a menudo diseñan sitios web fraudulentos que imitan al Banco de la Nación, pretendiendo ofrecer la gestión y solicitud digital del clave token. En estos

sitios falsos, se solicita información confidencial, como el número de tarjeta y la clave, que no es requerida por el banco legítimo. Basta con que la víctima proporcione estos datos en la página engañosa para que los estafadores puedan vaciar su cuenta bancaria.

En resumen, Villavicencio (2014) identifica las siguientes vulnerabilidades en el entorno digital:

i. Falta de una estructura jerárquica en la red, complicando el control y la verificación de la información en circulación.
ii. Creciente número de usuarios sin conciencia de los riesgos tecnológicos.
iii. El anonimato en internet, que complica la identificación de los responsables de delitos cibernéticos.
iv. El fácil acceso a la información, facilitando la alteración de datos y la destrucción de sistemas.

Además de lo ya dicho, es pertinente destacar, según la Defensoría del Pueblo (2023), que la Interpol, un organismo que integra a 194 cuerpos policiales internacionales, ha señalado seis factores clave que fomentan la ciberdelincuencia:

i. La creciente conectividad, dado que más personas se conectan en línea sin suficiente conciencia sobre seguridad digital, divulgando información personal.
ii. La movilidad, que incrementa las transacciones, comunicaciones y negocios en línea sin las adecuadas medidas de seguridad.
iii. La interconexión, que aumenta el número de dispositivos digitales vulnerables debido a la expansión de ciudades y hogares inteligentes.
iv. La sofisticación, que refleja la evolución constante de las habilidades y tácticas de los expertos en cibernética, quienes ofrecen servicios, incluso ilegales, a quienes paguen por ellos.
v. La falta de conocimiento sobre la magnitud y funcionamiento de este fenómeno, así como

la reticencia de las víctimas a denunciar por desconocimiento, desinterés, vergüenza, entre otras razones.

vi. La dificultad de las investigaciones complejas y transfronterizas necesarias para aclarar estos tipos penales por parte de las autoridades jurisdiccionales.

Es fundamental destacar que en el 12º Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal se discutieron varios mecanismos y recursos legales cruciales. En este contexto, es necesario subrayar la importancia de contar con herramientas legales adecuadas, dado que la eficacia de la ley depende en gran medida de la disponibilidad de recursos para la investigación. Por ejemplo, los programas informáticos forenses que permiten la recopilación de pruebas, el registro de pulsaciones del teclado y la recuperación de archivos eliminados son esenciales. También es crucial disponer de software y bases de datos para gestionar investigaciones, así como integrar características como el "hash" para imágenes de pornografía infantil (Espinoza Calderón, 2022).

Los crímenes cibernéticos se llevan a cabo utilizando tecnologías digitales sofisticadas, por lo que quienes investigan estos crímenes deben tener acceso a herramientas comparables a las que usan los criminales, y preferiblemente contar con equipos más avanzados, como software y hardware actualizados. Esto es crucial para combatir eficazmente la ciberdelincuencia, haciendo que la obtención de estos recursos sea esencial e inmediata para una respuesta adecuada ante este tipo de delitos.

Los crímenes en el ciberespacio se consideran una categoría emergente de delitos, comúnmente denominados delitos digitales o tecnológicos debido a su conexión directa con los avances científicos y tecnológicos (Villavicencio, 2014).

El derecho penal y las políticas de prevención del crimen se están ajustando a las transformaciones emergentes. Las tecnologías de la información y comunicación (TIC) están experimentando un rápido avance, y la criminalidad está cambiando junto con ellas. Hoy en

día, los crímenes se han mudado al entorno digital, que proporciona beneficios adicionales a los delincuentes: es más complicado localizarlos, no enfrentan riesgos físicos y la investigación de estos delitos se vuelve más compleja. (Espinoza Coila, 2014)

Las tácticas delictivas de los ciberdelincuentes se transforman constantemente, superando la delincuencia tradicional en complejidad y peligrosidad. Estos criminales apuntan principalmente a individuos vulnerables como ancianos, niños, o personas con conocimientos tecnológicos limitados. La ciberdelincuencia plantea un reto considerable para nuestro sistema judicial, así como para la policía, la fiscalía y los jueces, quienes frecuentemente son engañados por delincuentes con habilidades especializadas, mientras que los operadores del sistema penal carecen de formación en informática (Villavicencio, 2014).

Los delitos informáticos en Perú han sido abordados legalmente solo recientemente, ya que el Estado estuvo largo tiempo desentendido del problema. Sin embargo, la realidad lo ha llevado a actuar. Ahora, el Estado ha tenido que implementar medidas para enfrentar los ciberdelitos, aunque estas aún presentan algunas deficiencias. No obstante, este es un primer paso importante. Así, el Gobierno ha empezado a emitir normas relacionadas con el gobierno digital, la protección de datos y la virtualización de servicios públicos y privados. Además, se han designado autoridades para asegurar el cumplimiento de estas regulaciones.

En el pasado, los ciberdelitos solían afectar principalmente a grandes corporaciones, tanto del sector público como privado, destacando especialmente los bancos. Sin embargo, en la actualidad, cualquier familia o pequeña empresa que utilice sistemas informáticos puede convertirse en víctima de estos delitos. Así, se observa un cambio en el perfil de las víctimas, que ahora incluyen a individuos comunes y no solo a grandes empresas. Por esta razón, los ciberdelincuentes se enfocan en áreas con alta densidad poblacional y actividad comercial constante (Veiga, 2003).

Es crucial observar que el aumento de delitos informáticos se manifiesta a nivel global,

nacional y local. Diversos factores contribuyen a este fenómeno, aunque su impacto varía según la región específica. Una razón común es la creciente dependencia de la tecnología por parte de las personas, combinada con el rápido avance y la proliferación de nuevas tecnologías, así como la adopción de estilos de vida modernos (como la educación y los pagos virtuales) que se han vuelto habituales (Aguilar, 2013).

García-Peñalvo y Mendes (2023) sostienen que el progreso tecnológico ha dado lugar a un incremento en los crímenes digitales perpetrados mediante las tecnologías de la información y comunicación (TIC). Estos delitos pueden afectar considerablemente tanto a individuos como a entidades, y se prevé que el desarrollo tecnológico seguirá fomentando el auge de estos delitos. Por lo tanto, es crucial que tanto las personas como las organizaciones implementen estrategias para resguardarse de estos riesgos.

La investigación sobre ciberdelincuencia en países en desarrollo está en sus primeras etapas. Según la literatura, esto se debe a la percepción de que en muchas de estas naciones aún existe una significativa brecha digital o que la adopción de Internet es limitada. Kshetri (2010) lo menciona. Esta falta de interés ha llevado a que se asignen escasos recursos para enfrentar el cibercrimen, ya que durante mucho tiempo no se ha considerado una amenaza real. Sin embargo, la alta pobreza y el desempleo en estos países han incentivado a algunos a incurrir en estos delitos, al ofrecer oportunidades para delinquir con bajos costos. Por ejemplo, un hacker puede aprender a robar contraseñas solo con una computadora y una conexión estable a Internet.

La ausencia de medidas efectivas contra el cibercrimen complica la identificación y el castigo de los delincuentes informáticos (Kshetri, 2010), lo que incrementa las oportunidades de los criminales de beneficiarse de sus actividades. En países en desarrollo como Perú, donde la digitalización de transacciones está en sus primeras etapas, tanto consumidores como empresas aún no implementan las adecuadas medidas de ciberseguridad. Esta falta de

protección eleva el riesgo y la recompensa para los delincuentes. Además, Mora (2015) destaca una carencia significativa de personal capacitado en el uso de TIC en las comisarías peruanas, dejando a los oficiales en desventaja frente a los delincuentes. La situación es aún más crítica en las comisarías fuera de las principales ciudades.

Es crucial considerar la decisión de reportar un ciberdelito en Perú. Según Leukfeldt (2017), los factores económicos influyen en la elección de denunciar un cibercrimen, ya que involucra costos y beneficios. En el caso del Perú, presentar una denuncia por un delito informático podría generar altos costos, como el tiempo y los recursos necesarios, mientras que los beneficios serían escasos, dado que la posibilidad de identificar y sancionar al delincuente es muy baja. Además, el estudio indica que la policía en países de ingresos medios carece de las habilidades y conocimientos necesarios para gestionar eficazmente los casos de cibercrimen.

Dado lo que se ha expuesto anteriormente, resulta crucial considerar el posible regreso del delincuente para evaluar cómo el uso de las TIC en las comisarías podría impactar en dicho regreso. Según Ngafeeson (2010), cuando se comete un delito informático, los infractores enfrentan una barrera de seguridad que afecta directamente las probabilidades de ser capturados o de quedar impunes. Esta barrera de seguridad se basa tanto en las medidas de ciberseguridad que pueden implementar empresas o individuos, como en las capacidades tecnológicas de la comisaría. En este sentido, Ortiz (2013) destaca que la tecnología puede potenciar enormemente las habilidades de los agentes en la captura, análisis e investigación, siendo especialmente relevante para los ciberdelitos, ya que estos se cometen utilizando principalmente las TIC.

El vertiginoso avance y la adopción masiva de las Tecnologías de la Información y la Comunicación (TIC) han provocado cambios profundos en la sociedad, marcando un claro contraste con el entorno social de hace quince años. Estos cambios son sistemáticos y rápidos,

ofreciendo continuamente nuevas formas de ver el estilo de vida. Los humanos, como seres adaptables, integran la tecnología emergente en su rutina diaria, buscando mejorar la sociedad. No obstante, es esencial garantizar que estas acciones respeten los derechos de los demás. Mientras se mantengan dentro del marco legal, estas actividades pueden realizarse sin problemas. Sin embargo, la utilización de Internet y medios electrónicos para actividades criminales o infracciones representa una amenaza seria para la sociedad, exigiendo sanciones adecuadas. Esta conducta perjudicial se conoce comúnmente como delito informático, ciberdelito o ciberdelincuencia.

Rayon y Gomez (2014) definen el término "ciberdelito" como cualquier conducta criminal que acarrea consecuencias legales. Este tipo de delito se caracteriza por el uso de tecnología informática o de Internet, ya sea como herramienta para cometer el delito o como el propio objetivo del mismo. La aparición de la tecnología informática ha permitido a las organizaciones criminales acceder y utilizar estas herramientas modernas para llevar a cabo actividades ilegales. En este contexto, el perpetrador suele ser una persona con conocimientos avanzados en Tecnologías de la Información, que forma parte de redes criminales y posee un alto nivel de experiencia y formación, lo que frecuentemente pone en riesgo su ciberseguridad.

El ciberdelito moderno representa un gran obstáculo para su persecución, principalmente porque resulta difícil identificar con precisión a los culpables. Este problema se agrava aún más por la escasa cooperación entre los actores involucrados. No obstante, es importante destacar que el ciberdelito a menudo resulta ser una actividad mucho más rentable que el tráfico de drogas, moviendo millones de dólares cada año. Según Quinteros, el cibercrimen tiene una jurisdicción global, lo que implica que tanto los delincuentes como los proveedores de servicios pueden estar ubicados en diversas regiones. Así, el problema principal no es la falta de leyes o jurisdicción, sino la necesidad de establecer un tribunal adecuado para juzgar estos delitos.

En la clasificación de la ciberdelincuencia, se considera que esta puede aparecer como un medio o como un elemento físico. Zegarra (2015) explica que el comportamiento criminal que emplea computadoras e internet como herramientas se inscribe en el ámbito de los medios de comunicación. Es crucial destacar que cuando se menciona el uso de estos medios como herramientas, se alude a su empleo en la perpetración de delitos, siendo frecuentemente los delitos convencionales los objetivos finales. Además, especifica que los delitos dirigidos contra las computadoras, o sea, contra la tecnología de la información, se catalogan como delitos contra objetos materiales.

Diversos expertos han presentado distintas formas de clasificar los delitos informáticos. Sin embargo, según Téllez, citado por Gil (2007), la clasificación de Téllez se ajusta mejor a los objetivos de nuestra investigación.

Los delitos informáticos abarcan una variedad de actos ilegales que emplean tecnologías de la información y comunicación (TIC) como herramienta o método. Estos actos abarcan la falsificación engañosa de documentos digitales, tales como títulos, derechos de propiedad intelectual, tarjetas de crédito, cheques, y la modificación de registros económicos en los sistemas contables empresariales. También se extienden a la planificación y ejecución de delitos tradicionales adaptados a entornos digitales, como robo, homicidio, fraude, explotación infantil, trata de personas, pornografía infantil y fraude financiero, entre otros.

Los delitos informáticos abarcan acciones delictivas dirigidas específicamente a computadoras, sus componentes o software como objetos físicos. Un ejemplo en el ámbito de la programación es cuando un sistema deja de funcionar por completo. Esto incluye la eliminación de bases de datos empresariales, la manipulación no autorizada de servidores corporativos, y la interrupción de programas hasta volverlos inoperables. También se incluyen ataques físicos a los equipos o sus componentes, así como actos de sabotaje o terrorismo que destruyen o toman control de sistemas computarizados clave. Otro ejemplo es la apropiación

de medios magnéticos que contienen información valiosa, utilizada para extorsionar a personas u organizaciones, normalmente mediante demandas de rescate u otras formas de chantaje.

Según López (2013), la tipicidad se refiere a la cualidad que se le atribuye a un comportamiento cuando este se ajusta al modelo de un delito específico (p. 53). Es decir, implica que la acción en cuestión cae dentro del ámbito penal al incorporar los elementos que definen dicho marco jurídico. Es importante diferenciar entre el tipo objetivo, que se centra en la acción en sí misma, y el tipo subjetivo, que se relaciona con la intención o la culpa del individuo. El legislador no solo proporciona una descripción objetiva de la conducta sancionable, sino que también presenta fundamentos y evidencias que respaldan su carácter ilícito.

Este estudio tiene como propósito identificar las características distintivas de los delitos informáticos, los cuales han emergido a raíz del desarrollo de las tecnologías de la información, generando así nuevas formas de comportamiento delictivo.

El concepto de tipicidad busca establecer los parámetros exactos que permiten identificar cuándo la afectación de un bien jurídico es consecuencia directa de la conducta de una persona, en lugar de ser simplemente un resultado casual. Se llevó a cabo un examen de la norma para identificar la tipicidad objetiva en los delitos informáticos, evaluando diversos aspectos como el objeto del delito, los actores involucrados, la acción típica ejecutada, la relación de causalidad, la imputación objetiva y los elementos descriptivos normativos que caracterizan este tipo de delitos.

De acuerdo con Hurtado (2005), el blanco del delito se refiere a la persona o entidad hacia la cual se dirige la acción ilegal. Esto incluye a todas las entidades que son el objetivo o propósito de la actividad delictiva. En el contexto de la criminalidad informática, se pueden identificar diversas categorías que incluyen delitos vinculados a datos y sistemas informáticos, agresiones contra la autonomía sexual y la libertad individual, infracciones a la privacidad y

confidencialidad de las comunicaciones, delitos contra la propiedad y violaciones a la confianza pública.

Según Hurtado (2005), la acción descrita por el verbo principal en la norma jurídica constituye el núcleo esencial del aspecto objetivo dentro de la categoría jurídica. En esencia, es este verbo el que delimita la conducta contemplada por la ley.

Es esencial identificar a cualquier persona que busque ser parte de un grupo colectivo. En el contexto actual, el foco de nuestro análisis recae en aquellos involucrados en la realización de actos delictivos. Aquí, se distinguen tanto un agente que actúa como otro que es afectado.

Según Valdez y Lima, citados por Gil (2007), el Sujeto Activo en la ciberdelincuencia es una persona que no se ajusta al perfil convencional de un delincuente. Se caracteriza por poseer habilidades especializadas en la gestión de sistemas informáticos y ocupar posiciones estratégicas que les permiten acceder a información confidencial. Además, su habilidad en el manejo de tecnología informática les permite operar de manera discreta, utilizando códigos numéricos y lógica binaria, lo que los hace difíciles de identificar. Esta capacidad excepcional ha generado debates éticos y educativos, con propuestas para limitar el acceso a estos conocimientos.

Los ataques cibernéticos puros se caracterizan por el uso de tecnologías emergentes tanto como herramientas como objetivos, mientras que los ataques cibernéticos replicados involucran la aplicación de estas nuevas tecnologías para ejecutar crímenes tradicionales. Propongo que la relación entre los delitos cibernéticos y aquellos vinculados a la propiedad intelectual, también conocidos como "delitos contra los derechos intelectuales" según el Código Penal, se enmarca en esta segunda categoría. La adopción de nuevas tecnologías, como el Internet, el desarrollo de software y la creación de plataformas de comunicación masiva, facilita la comisión de delitos que ya existían antes de su adopción generalizada.

El sujeto que habitualmente se considera como el perpetrador del ciberdelito es a menudo quien lleva a cabo la acción ilegal. Giménez (2011) señala que aquellos que se involucran en delitos informáticos suelen ser individuos con roles de confianza, como empleados que tienen acceso autorizado a sistemas informáticos. Los datos estadísticos revelan que más del 90% de estos delitos son cometidos por personas que tienen un conocimiento profundo y están familiarizadas con el sistema, mientras que los técnicos informáticos participan en un porcentaje menor de los casos.

Esto indica que las personas involucradas en delitos informáticos suelen tener un acceso sencillo a estos sistemas y un conocimiento profundo de sus fallas y puntos débiles. Su habilidad para sortear las protecciones de seguridad les facilita recuperar o eliminar la información que necesitan.

Respecto a la categoría del fraude informático, Riquert (2020) lo describe como una acción u omisión significativa desde el punto de vista penal, llevada a cabo a través de medios informáticos o dirigida contra sistemas informáticos de terceros. De manera similar, González (2017) argumenta que el delito informático es cualquier conducta punible que utiliza o tiene como objetivo técnicas informáticas, y que, al ser vulneradas, perjudica los derechos de personas físicas o jurídicas en favor del autor del delito.

El fraude informático a menudo se considera el pilar de la cibercriminalidad, una práctica que desde sus comienzos ha estado vinculada a la transferencia electrónica no autorizada de dinero (Department of Justice, 2016). Este término abarca una variedad de conductas, cuyas complejidades terminológicas, y técnicas han evolucionado con el tiempo, adaptándose a los avances tecnológicos y a las nuevas formas de interacción en el entorno digital. La creciente sofisticación de las tácticas empleadas por los delincuentes informáticos ha llevado a una mayor dificultad en la detección y prevención de estos delitos, lo que a su vez ha impulsado el desarrollo de herramientas y estrategias más avanzadas por parte de las

instituciones financieras y las agencias de seguridad. Además, el fraude informático no solo afecta a individuos y empresas, sino que también puede tener repercusiones significativas en la estabilidad económica y en la confianza en los sistemas financieros globales. Por lo tanto, abordar este problema requiere una colaboración estrecha entre entidades gubernamentales, sector privado y el público en general para fortalecer la ciberseguridad y proteger los activos digitales de los usuarios. Según Villegas (2018), se pueden resumir de la siguiente manera:

El concepto de fraude informático frecuentemente está relacionado con acciones tentativas o incompletas, así como con actos preparatorios de un fraude en su definición más estricta. Según Martínez y Devia (2019), el fraude informático no se considera un delito en sí mismo, sino más bien una fase preliminar que se vuelve relevante desde el punto de vista penal cuando compromete la seguridad de la información en sistemas informáticos. Ejemplos de tales actividades preliminares, como el phishing y el pharming, están asociados con operaciones bancarias indebidas y se clasifican como fraude informático.

El delito de fraude informático a menudo está relacionado con el hacking, ya que su ejecución generalmente implica el acceso no autorizado a datos dentro de sistemas informáticos (Grisales, 2020).

Por otro lado, Vizcardo (2017) señala que una corriente importante en la doctrina aún utiliza el término "delito informático" para englobar acciones como el robo realizado a través de medios electrónicos y ataques contra sistemas y datos informáticos. Según esta perspectiva, el delito informático puede variar en su naturaleza y estructura, y los bienes jurídicos que protege no siempre son los mismos, reflejando la diversidad y la dinámica de los riesgos asociados con el entorno digital. Esta visión sostiene que el "delito informático" no es una categoría uniforme, sino que abarca una serie de conductas delictivas que pueden impactar diferentes aspectos de la seguridad informática. Por ejemplo, el robo de identidad, el espionaje cibernético y el sabotaje de sistemas críticos son manifestaciones distintas de esta categoría

general, cada una con sus propias implicaciones legales y técnicas. Así, la clasificación y el tratamiento de estos delitos requieren un enfoque flexible y adaptativo, capaz de integrar los constantes cambios en la tecnología y las metodologías utilizadas por los delincuentes. Esta perspectiva subraya la necesidad de una legislación y una práctica judicial que evolucionen paralelamente con el desarrollo tecnológico para garantizar una protección efectiva contra el espectro amplio y en constante cambio de los delitos informáticos (Garcés et al., 2020).

En resumen, los delitos informáticos están estrechamente relacionados con el uso de dispositivos tecnológicos como computadoras, internet, celulares o tabletas para cometer actos ilícitos. Estos delitos pueden servirse de la tecnología tanto como herramienta para perpetrar acciones ilegales como su objetivo final (Villavicencio, 2014, p. 49). En esencia, los delitos informáticos consisten en actividades contrarias a la ley que emplean equipos tecnológicos para alcanzar diversos propósitos, siempre con la intención de vulnerar algún bien jurídico. Es importante destacar que estas acciones ilegales ocurren en el ciberespacio, un ámbito virtual creado por la red o internet a través de dispositivos tecnológicos.

García destaca que una de las formas más frecuentes de cibercrimen implica la transferencia de bienes patrimoniales hacia el perpetrador del delito (2008). De manera similar, Delgado (2016) menciona que este delito se basa en la manipulación de sistemas informáticos, aprovechando las repeticiones automáticas inherentes a la tecnología. En países como México, es conocido como la "técnica del salchichón". Este término surge porque, cuando existen activos patrimoniales almacenados en la red, los delincuentes los sustraen en pequeñas cantidades casi imperceptibles para los propietarios, lo que evita sospechas sobre el crimen y permite al delincuente cumplir con su propósito. Así, el fraude informático se caracteriza por un engaño que induce a error a terceros, resultando en la adquisición de bienes a expensas de estos.

Según Espinoza cualquier persona con conocimientos básicos de informática puede ser

el autor de un delito informático, lo que incluye a gamers, empleados bancarios, operadores telefónicos, entre otros (2022). De manera similar, Josefina García sostiene que estos individuos también pueden ser aquellos con acceso autorizado a sistemas, siempre y cuando utilicen la tecnología para obtener un beneficio personal.

Según Espinoza (2022), cualquier individuo o entidad, especialmente aquellos con limitados conocimientos en informática, como los ancianos y los niños, puede ser objetivo de este tipo de delito. En otras palabras, este individuo es quien posee o tiene la titularidad del bien que ha sido perjudicado.

Según Acuario (2016), en Alemania, la legislación que penaliza los actos ilícitos en el ámbito de la informática entró en vigor en 1986. Sin embargo, fue cuando se promulgó la ley que aborda la Criminalidad Económica, estableciendo como delitos el espionaje de datos, el fraude informático, la falsificación de datos probatorios y otros documentos destinados a engañar en el tráfico jurídico, la manipulación de datos, el sabotaje informático, y el uso indebido de cheques o tarjetas de crédito.

Según Valmaceda (2011), en este país la interpretación jurídica predominante considera que, para que un acto sea clasificado como fraude dentro del tipo penal, es necesario que implique un "engaño" dirigido a otra persona, similar al concepto de estafa. En otras palabras, un acto solo se consideraría fraudulento si resulta en un perjuicio directo al patrimonio de la víctima. En cuanto al phishing, existen múltiples variantes en Internet, caracterizadas por una gran diversidad en sus métodos y estrategias. Mariana (2021) señala que la forma más común de phishing en la actualidad es el envío masivo de correos electrónicos, cuyo objetivo principal es obtener información personal y financiera de usuarios desprevenidos.

Dado que el phishing evoluciona de manera continua, diversos estudios han identificado una serie de etapas en la perpetración de este delito. Sin embargo, estas etapas pueden diferir según el tipo de ataque, la dificultad, la sofisticación, la habilidad del atacante y

la implicación de la víctima. En este contexto, Mayra Mariana identifica seis fases distintas.

2.2.1. Planificación

En esta fase, el ciberdelincuente se dedica a organizar y planear su ataque. Es aquí donde selecciona a su víctima, decide la modalidad del ataque, el tipo de phishing que utilizará, y determina el número de víctimas y cómplices involucrados. También define si el objetivo será una persona física o jurídica. En esencia, esta fase corresponde a la parte interna del "Iter Criminis", donde el delincuente reflexiona sobre si cometerá el crimen y cómo llevará a cabo su plan malicioso.

2.2.2. Preparación

Mariana señala que, en esta etapa, la intervención externa es mínima. El ciberdelincuente se concentra en los objetivos del delito, los medios que utilizará y los mecanismos necesarios. Por ejemplo, el enfoque de un correo de phishing variará si está dirigido a una persona específica o a un grupo. Un correo personalizado será más detallado y adaptado a la víctima, mientras que uno dirigido a un grupo será más genérico. Esta fase corresponde a los Actos Preparatorios, ya que las acciones que se realizan aún no constituyen la ejecución del delito y tienen un contenido delictivo limitado.

2.2.3. Ataque

Durante esta fase, los criminales cibernéticos comienzan a desplegar diversos ataques de phishing utilizando las herramientas tecnológicas más adecuadas para sus objetivos. El grado de participación de la víctima, ya sea bajo, medio o alto, juega un papel crucial en esta etapa, ya que influye en la complejidad del ataque. Según Mariana (2021), en este punto se analiza detalladamente la “anatomía del phishing”, que consta de siete componentes clave: el malware, la infección, la ejecución, la recopilación de datos, el atacante y el servidor legítimo. Además, se identifican dos fases críticas en la infección: la contaminación del dispositivo tecnológico y la activación del código malicioso. Esta etapa se considera tentativa, dado que el

perpetrador ya ha comenzado a llevar a cabo el delito.

2.2.4. Fase de adquisición de información

En esta fase, el atacante aguarda a que el software malicioso comience a extraer datos personales y detalles cruciales que le permitan acceder a los bienes de las víctimas. La duración de este proceso varía según el grado de involucramiento de las víctimas: si la participación es baja, el tiempo requerido será menor; con una participación moderada, el tiempo se extenderá; y si la implicación es alta, el proceso será aún más prolongado. Este lapso se considera la consumación del delito, ya que es cuando el perpetrador logra cumplir con el plan previamente establecido.

2.2.5. Desarrollo

En esta fase, el criminal cuenta ya con la información de las víctimas. Aquí, el delincuente determina si usará toda la información en su propio beneficio o la venderá a otros para que ellos cometan los delitos. En esta etapa, el delincuente busca alcanzar el objetivo que se había propuesto.

2.2.6. Realización

Momento en que el autor del delito ya ha recopilado la información de las víctimas. En esta fase, el criminal decide si utilizar todos los datos en su propio beneficio o venderlos a terceros para que ellos cometan los delitos. Aquí, el perpetrador busca lograr el objetivo que se propuso.

Las subcategorías del fraude informático incluyen el tipo de hurto realizado mediante medios electrónicos. Según las teorías predominantes, Pedrera et al. (2007) sugieren que el delito de fraude informático protege dos bienes jurídicos principales: a) la confidencialidad, seguridad e integridad de los datos e información almacenados en soportes informáticos, y b) el patrimonio.

Ambas definiciones pueden ser cuestionadas por su excesiva amplitud, vaguedad y

ambigüedad, ya que no se centran en un bien jurídico específico. Mientras algunas conductas afectan la confidencialidad de la información en sistemas informáticos, otras, como el robo mediante medios electrónicos, atacan el patrimonio. Además, hay delitos que pueden comprometer la integridad y libertad sexual de menores a través del tráfico de pornografía en línea (Utreras, 2017).

Aunque el término "delito informático" se traduce del anglosajón "computer crime", estas definiciones suelen ser imprecisas y no encajan claramente en ninguna categoría jurídico-penal específica. Algunos incluso argumentan que el concepto de delito informático, en rigor, no existe (Song et al., 2016). Al examinar la legislación nacional, se observa que la Ley N°30096, conocida como la "Ley de Delitos Informáticos", clasifica estos delitos según el bien jurídico protegido. Según esta ley, los delitos informáticos se dividen en: a) delitos contra datos y sistemas informáticos; b) delitos contra la indemnidad y libertad sexual; c) delitos contra la intimidad y el secreto de las comunicaciones; d) delitos contra el patrimonio; y e) delitos contra la fe pública.

Morales (2018) sostiene que, aunque los delitos informáticos pueden proteger diversos bienes jurídicos, el fraude informático está dirigido principalmente a proteger el patrimonio. No obstante, según Pardo (2018), aunque el objetivo del perpetrador sea económico, la ejecución del delito implica una violación de los datos personales de la víctima en sistemas informáticos. Esto sugiere la posibilidad de que se produzca un conflicto entre diferentes normas penales o tipos de delitos.

En concordancia con lo anterior, el fraude informático, como delito relacionado con el patrimonio, está regulado en el Capítulo V, artículo 8 de la Ley N°30096. Esta ley establece penas de entre tres a ocho años para quienes, utilizando tecnologías de la información y comunicación (TIC), obtengan beneficios patrimoniales para sí mismos o para otros. El aspecto clave de estos delitos incluye el diseño, introducción, modificación, eliminación, duplicación

de información digital, así como cualquier alteración o intervención en el desempeño de los sistemas informáticos. Por otra parte, Calvo (2014) menciona que el comportamiento requerido por la norma es crucial para formular un juicio crítico hacia el individuo que actúa en contra de lo establecido por la ley.

El hurto informático se define como la apropiación indebida de recursos económicos de una persona por medio de la alteración, manipulación o robo de información confidencial almacenada en sistemas informáticos. Así, se argumenta que este delito primero compromete la confidencialidad de los datos y luego permite la sustracción del patrimonio de la víctima, ya sea para beneficio propio o de terceros.

Arbulú (2019) reflexiona sobre que, según quienes apoyan esta teoría, el robo de dinero a través del acceso a sistemas bancarios en línea o sitios web de instituciones financieras se clasificaría como un cibercrimen. Para esta perspectiva, lo crucial no es el bien jurídico protegido, sino que el delito se comete utilizando medios informáticos (Bocij, 2015). De acuerdo con Tejero (2019), bajo esta concepción, cualquier actividad ilegal que pueda realizarse mediante medios cibernéticos podría ser considerada un cibercrimen.

Sánchez (2017) argumenta que clasificar el fraude informático como un delito separado del hurto no fue la decisión adecuada, ya que, en esencia, solo se está reconociendo un "nuevo" método para cometer hurto dentro de una categoría penal independiente. Según esta visión, no es necesario crear un tipo penal autónomo simplemente porque el delito se lleva a cabo a través de un nuevo medio, como la alteración o violación no autorizada de sistemas informáticos.

Se ha argumentado que, dado que el fraude informático no es más que un hurto llevado a cabo a través de medios electrónicos, al igual que el legislador nacional, el bien jurídico protegido por este delito es el patrimonio. En términos de análisis típico, el único aspecto en el que el fraude informático se diferencia del hurto es en la forma en que se lleva a cabo la acción, que requiere que el delincuente use técnicas como el diseño, introducción, alteración,

eliminación, supresión o clonación de datos informáticos, así como cualquier tipo de interferencia o manipulación de los sistemas informáticos.

En cuanto a los aspectos subjetivos del tipo penal, Medina y Herrada (2017) sostienen que tanto el fraude informático como el hurto son delitos que se cometen con dolo, con el objetivo exclusivo de obtener un beneficio patrimonial indebido, ya sea para el propio autor o para un tercero. Así, dado que ambos delitos son delitos de resultado, si el delincuente no logra obtener un "beneficio económico", la conducta se considera atípica, ya que no se ha producido un provecho económico para el autor del delito cibernético.

Esto significa que, si el beneficio no se obtiene a través de la violación o alteración de datos en sistemas informáticos, sino por otros medios, el autor será responsable de un delito de hurto (simple o agravado) y no de fraude informático. Esto demuestra que, según el artículo 8 de la Ley N°30096, lo que se define como "fraude informático" no es más que un hurto realizado mediante medios electrónicos.

En cuanto al **derecho al patrimonio**, cualquier vulneración de este derecho implica la transgresión de las protecciones consagradas en la constitución. Este tipo de transgresión, que se denomina delito informático, atenta contra el derecho patrimonial, impactando en posesiones personales tales como efectivo, bienes tangibles, dispositivos tecnológicos, alimentos, mobiliario, inmuebles y otros recursos (Huamán, 2020).

Además, la vulneración del derecho al patrimonio a través de delitos informáticos no solo afecta directamente los bienes materiales y financieros, sino que también puede generar efectos colaterales significativos en la estabilidad emocional y psicológica de las víctimas. El robo de identidad, por ejemplo, puede llevar a la pérdida de confianza en los sistemas de seguridad y causar estrés prolongado mientras se intenta recuperar la identidad y reparar el daño. Asimismo, los ataques cibernéticos que comprometen información personal o empresarial pueden acarrear efectos desastrosos, como la eliminación de información valiosa

hasta daños irreparables en la reputación. En este contexto, la protección del patrimonio en el ámbito digital se convierte en una cuestión multifacética que requiere una respuesta integral, incluyendo medidas preventivas robustas, mecanismos efectivos de recuperación y una actualización constante de las normativas para enfrentar las nuevas formas de criminalidad tecnológica.

En el ámbito del patrimonio, Arias (2017) afirma que la noción de víctima se refiere a la persona que sufre perjuicios a causa de actos delictivos. García (2019) señala que los bienes jurídicos protegidos incluyen la propiedad y la privacidad personal; sin embargo, numerosos especialistas creen que los delitos informáticos afectan una variedad de bienes protegidos y otros que podrían requerir protección en el futuro debido a la evolución de las formas de criminalidad. Además, Morena del Río (2020) subraya la importancia de salvaguardar los bienes jurídicos dentro del marco normativo administrativo, asegurando así la seguridad de los intereses de los propietarios.

Y la integridad de sus derechos en un entorno digital en constante cambio. Esta perspectiva resalta que, a medida que la tecnología avanza, emergen nuevos bienes jurídicos susceptibles de ser vulnerados, lo que plantea desafíos adicionales para el marco legal vigente. Verbigracia, la tutela de datos personales y la integridad de los sistemas de información se han vuelto en aspectos críticos, dada la creciente dependencia de plataformas digitales en la vida cotidiana y empresarial. Además, la adaptación del marco normativo administrativo debe ser dinámica, incorporando no solo las amenazas actuales, sino también anticipándose a las posibles innovaciones en la criminalidad cibernética. Así, asegurar que la legislación evolucione en consonancia con estos cambios es esencial para asegurar una tutela eficiente de los derechos patrimoniales y personales, evitando lagunas legales que puedan ser explotadas por los delincuentes.

Desde una perspectiva diferente, el **daño moral** se refleja en la frustración por no

recibir las ganancias anticipadas, la disminución del capital y las tensiones psicológicas resultantes de las pérdidas económicas. No se limita a un problema financiero, sino que afecta al bienestar emocional del individuo. Según Collque (2017), esto se evidencia en alteraciones emocionales como tristeza profunda, ansiedad, enojo, temor, agresividad, inseguridad y desmotivación, entre otras emociones contradictorias.

Estas consecuencias emocionales pueden ejercer una influencia intensa y prolongada en la existencia de las víctimas, afectando su capacidad para llevar una vida equilibrada y satisfactoria. La pérdida económica provocada por delitos informáticos no solo puede desestabilizar las finanzas personales o empresariales, sino que también puede erosionar la autoestima y la percepción de seguridad. La ansiedad y el miedo resultantes pueden influir en la toma de decisiones y en la capacidad de participar plenamente en actividades cotidianas. Collque (2017) subraya que estos efectos secundarios no siempre son reconocidos o compensados adecuadamente dentro del sistema legal, lo que pone de relieve la necesidad de una mayor sensibilidad hacia el daño moral en la evaluación de casos relacionados con delitos informáticos. En consecuencia, es crucial que las políticas de compensación y asistencia para víctimas consideren no solo la reparación de daños financieros, sino también el apoyo necesario para enfrentar y superar las secuelas emocionales y psicológicas que estos delitos pueden ocasionar.

En relación con el marco legal peruano, la Constitución en su Artículo 2, inciso 6, garantiza que todas las personas tienen derecho a acceder a servicios informáticos, tanto públicos como privados, siempre que estos no vulneren la privacidad personal y familiar. Aunque nuestra Constitución apoya el uso de la tecnología y la protección de la privacidad, no aborda específicamente el derecho a la protección frente al fraude informático que perjudica la propiedad de los usuarios de internet. Por lo tanto, existe una laguna legal en cuanto a la protección del patrimonio frente a delitos informáticos.

La Ley de Delitos Informáticos, Ley N° 30096, en su Artículo 8, define el fraude informático como un delito punible con prisión de 3 a 8 años. Si el fraude afecta a bienes de instituciones públicas dedicadas a servicios sociales, como albergues para ancianos, centros para discapacitados, orfanatos o comedores populares, la pena se incrementa a entre 5 y 10 años de cárcel. Además, el Código Penal Peruano, en su Artículo 245, aborda el ocultamiento, la omisión o la falsificación de información.

En general, son los gestores de bancos, entidades financieras y organismos públicos o privados quienes realizan estas actividades a través de medios digitales. Estos actos están penados con prisión de 4 a 8 años. Además, el Artículo 230 de nuestro Código Procesal Penal abarca la intrusión, la grabación de conversaciones por teléfono u otros métodos de comunicación, y la localización geográfica de teléfonos inalámbricos. También se incluye la obtención de datos de archivos informáticos, ya sean privados o públicos, mediante intervención fiscal, así como el levantamiento de documentos y archivos informáticos, regulado por los Artículos 231, 232, 233 y 234.

En contraste, después de examinar teorías científicas, Peña y Almanza (2010) argumentan en su libro sobre la teoría del delito que el funcionalismo moderado de Claus Roxin, jurista alemán, respalda la idea de que las clasificaciones del delito ofrecidas por el finalismo (tipicidad, antijuridicidad, culpabilidad) deben tener un enfoque político-criminal. Esto se debe a que los fundamentos de la punibilidad deben alinearse con los objetivos del Derecho penal. En esencia, estas categorías jurídicas sirven como herramientas para una evaluación político-criminal. Si un estado carece de una política criminal que integre la prevención del delito, la administración de justicia y la readaptación social, estará destinado a fracasar en su lucha contra la delincuencia.

Arias (2021) expone que la teoría del delito, cuando se aplica al ciberdelito, ofrece un marco teórico que ayuda a identificar que una acción realizada por un individuo es

precisamente esa acción. De manera similar, Espinoza (2022), desde Perú, en su obra sobre Delitos Informáticos y nuevas formas de criminalidad, señala que, en el fraude informático, el **bien jurídico protegido es el patrimonio**, que se manifiesta en datos numéricos convertibles en dinero físico.

Tipicidad Objetiva se refiere a un acto **ilícito intencional**. En términos de **conducta**, incluye la creación, modificación, eliminación, pausa o duplicación de archivos digitales, o la gestión ilegal de estos, que resulta en perjuicio para otros. El sujeto activo puede ser cualquier individuo con habilidades en informática, empleados de instituciones financieras o bancarias, o trabajadores del sector de telecomunicaciones. El **sujeto pasivo** puede ser cualquier persona, particularmente aquellos con habilidades informáticas limitadas. **Tipicidad subjetiva** se manifiesta como dolo, con la intención de apropiarse de un bien o causar daño a otra persona.

Existen diversas modalidades de fraudes digitales: el **fraude en línea** ocurre cuando los delincuentes se aprovechan de la red para captar señales y acceder a datos privados, permitiéndoles realizar transacciones desde cualquier ubicación. El **fraude de identidad** implica la usurpación de datos personales como nombre, fecha de nacimiento, direcciones previas y actuales, números de teléfono y contactos. La **ciberextorsión**, por otro lado, utiliza identificaciones personales, fotos de familiares y detalles sobre la situación económica de la víctima para ejercer coacción, amenazas y chantajes con el fin de exigir dinero.

Los ataques de **malware** o virus pueden manifestarse de diversas maneras. Los **adwares** son programas que muestran anuncios engañosos con imágenes y sonidos que se reproducen de forma automático, luego cobran por el servicio o interfieren con el uso del dispositivo. El **spyware** recoge información sobre la navegación del usuario y datos personales o financieros de manera oculta, mientras que los **keyloggers** registran las pulsaciones del teclado para enviar esta información al delincuente. Los **gusanos** se propagan a través de redes, causando errores y un uso anormal del ancho de banda. Los **troyanos** se camuflan en programas

piratas, como software de oficina o antivirus, y transmiten información al atacante. El **ransomware** bloquea o limita el acceso a la información del usuario, exigiendo un rescate para desbloquear o descifrar los archivos del dispositivo. Las **botnets** son redes de dispositivos comprometidos que los delincuentes usan para enviar grandes cantidades de spam. Por último, las **apps maliciosas** son aplicaciones desconocidas en dispositivos móviles que solicitan permisos para acceder y controlar credenciales, imágenes, videos y otros datos del dispositivo.

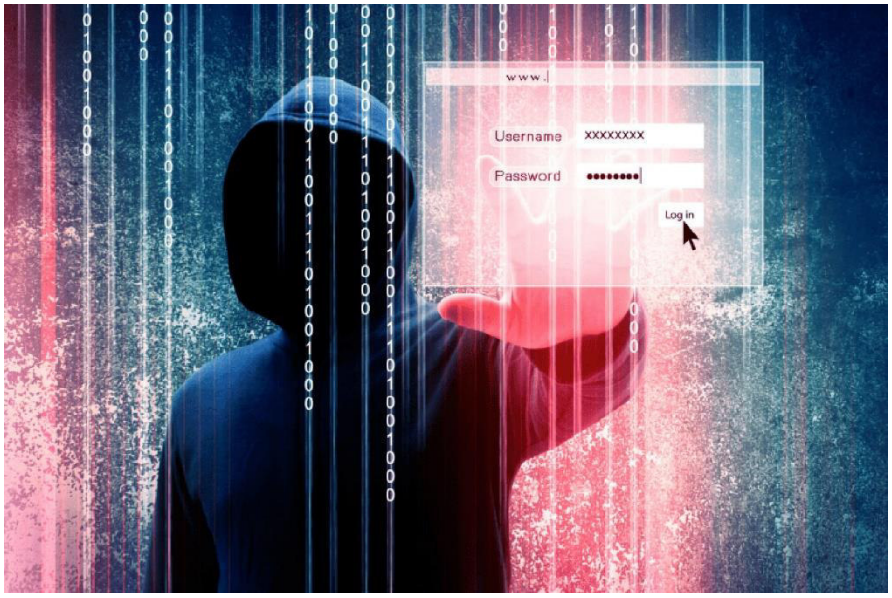
De acuerdo con la división de Investigación de Alta Tecnología (DIVINDAT) de la PNP y el Ministerio Público, las formas más frecuentes de fraude informático incluyen:

- Clonación de tarjetas de crédito: Delincuentes usan dispositivos electrónicos llamados skimmers para capturar la información de las tarjetas de crédito. Copian estos datos a una computadora y luego los transfieren a una tarjeta nueva, que se utiliza para solicitar créditos o realizar compras en línea.
- Phishing: Consiste en enviar correos electrónicos engañosos para dirigir a las víctimas a sitios web fraudulentos. Allí, los usuarios ingresan información personal, como números de tarjetas de crédito y contraseñas, que luego se usa para cometer fraude.
- Vishing: Combina el phishing con llamadas telefónicas falsas, donde los delincuentes imitan a una entidad bancaria para que la víctima revele su token digital o clave SMS para realizar transacciones fraudulentas.
- Smishing: Se envían mensajes de texto o WhatsApp falsos de un supuesto banco, alertando sobre una compra sospechosa. La víctima es instada a llamar a un número falso donde se le solicitan datos confidenciales.
- Carding: Compra en línea utilizando datos robados de tarjetas de crédito o débito, como el número de 16 dígitos, la fecha de vencimiento o el código de seguridad.
- Skimming: Utiliza un lector de códigos (skimmer) para captar rápidamente la información de las tarjetas de crédito.

- Pharming: Emplea software malicioso para redirigir a los usuarios desprevenidos a sitios web falsos, con el objetivo de recolectar datos personales.
- Keylogging: Instala un programa que registra todas las pulsaciones del teclado para obtener información sobre cuentas y datos personales.
- Sniffing: Aprovecha redes Wi-Fi públicas o no seguras para interceptar datos de clientes de entidades financieras o bancarias.

Figura 2

Sniffing: Técnica de seguridad informática utilizada para interceptar, capturar y analizar el tráfico de datos en una red, a menudo con fines maliciosos



III. MÉTODO

3.1. Tipo y diseño de investigación

El tipo de investigación utilizado es de enfoque, cuantitativo básico, El enfoque cuantitativo básico es un método científico que busca **medir y cuantificar la realidad** a través de **números y estadísticas** para probar hipótesis y teorías preestablecidas, analizando fenómenos de manera **objetiva y generalizable** mediante técnicas estructuradas como encuestas y experimentos, con el fin de establecer patrones y relaciones causales. (Muntané, 2010).

El diseño de nuestra investigación es **No Experimental, Transversal y Descriptivo - Correlacional.** Es no experimental porque no existe manipulación deliberada de las variables, sino que se observan los fenómenos tal como se dan en su contexto natural para analizarlos posteriormente. Es transversal debido a que la recolección de datos se realiza en un único momento temporal. Asimismo, el alcance es descriptivo-correlacional, pues busca especificar las propiedades importantes de las variables sometidas a análisis y evaluar la relación estadística existente entre ellas. Por ello, para llevar a cabo nuestra investigación bajo este diseño, se ha recurrido a la técnica de la encuesta, utilizando como instrumento un cuestionario estructurado

Nuestra investigación adoptó un enfoque **cuantitativo**, centrándose en un contexto complejo compuesto por diversas situaciones y eventos. Este enfoque nos permitió realizar un análisis detallado y reflexivo de los significados particulares que constituyen la realidad en estudio.

3.2. Población y muestra

3.2.1. Población

La población de estudio está conformada por los operadores jurídicos especializados en

materia penal (Jueces, Fiscales y Abogados Litigantes) que ejercen sus funciones dentro de la jurisdicción de la **Corte Superior de Justicia de Lima Norte** durante el periodo 2023. Según estimaciones basadas en la carga procesal y los directorios institucionales, se ha establecido una población finita aproximada de N= 1000 profesionales vinculados a delitos informáticos y patrimoniales.

Criterios de Inclusión:

Abogados habilitados por el Colegio de Abogados.

Fiscales y Jueces en ejercicio dentro del distrito judicial de Lima Norte.

Profesionales con experiencia o casos relacionados a delitos patrimoniales e informáticos.

Criterios de Exclusión:

Profesionales con licencias, suspendidos o que no litiguen en el área penal.

3.2.2. Muestra

La muestra se determinó mediante un **muestreo probabilístico aleatorio simple**, lo que garantiza que todos los elementos de la población tengan la misma probabilidad de ser seleccionados. Para el cálculo del tamaño muestral, se aplicó la fórmula estadística para poblaciones finitas con un nivel de confianza del 95% y un margen de error del 5%.

Fórmula aplicada:

$$n = \frac{Z^2 * p * q * N}{E^2 * (N-1) + Z^2 * p * q}$$

Donde:

n = Tamaño de la muestra buscada.

N = Tamaño de la población (1000).

Z = Nivel de confianza (1.96 para un 95% de seguridad).

p = Probabilidad de ocurrencia del evento (0.5 o 50%, máxima varianza).

q = Probabilidad de no ocurrencia ().

E = Margen de error máximo aceptable (0.05 o 5%).

Cálculo: Sustituyendo los valores en la fórmula:

$$n = \frac{1.96^2 * 0.5 * 0.5 * 1000}{(0.05^2) * (1000 - 1) + (1.96^2 * 0.5 * 0.5)}$$

$$n = \frac{3.8416 * 0.25 * 1000}{0.0025 * 999 + 3.8416 * 0.25}$$

$$n = \frac{960.4}{2.4975 + 0.9604}$$

$$n = \frac{960.4}{3.4579}$$

$$n = 277.74$$

Resultado: Ajustando al entero superior, la muestra requerida es de **encuestados**.

3.3. Operacionalización de variables

Las variables de estudio han sido desglosadas de conceptos teóricos a indicadores medibles para su análisis estadístico.

Variable 1: Fraude Informático (Variable Independiente)

Definición Conceptual: Se define como el acto ilícito realizado mediante la manipulación, alteración o supresión de datos en sistemas informáticos con el fin de obtener un beneficio económico indebido.

Definición Operacional: Será medida a través de un cuestionario que evalúa las dimensiones de: *Modalidades delictivas* (phishing, smishing, carding) y *Medios tecnológicos empleados* (TIC, clonación, software malicioso). Se utilizará una escala ordinal de tipo Likert.

Variable 2: Derecho al Patrimonio (Variable Dependiente)

Definición Conceptual: Facultad jurídica que tiene toda persona de proteger sus bienes económicos, ahorros y privacidad financiera frente a terceros.

Definición Operacional: Se medirá a través de la percepción de los operadores jurídicos sobre la afectación causada, evaluando las dimensiones de: *Daño Material* (pérdida económica

directa) y *Daño Moral* (afectación psicológica y seguridad jurídica)

3.4. Técnicas e instrumentos de recolección de datos

Para el presente estudio cuantitativo, se han definido los siguientes mecanismos:

Técnica: La técnica empleada fue la **encuesta**, la cual permite obtener información estandarizada de una muestra representativa de la población de estudio (abogados y operadores de justicia de Lima Norte).

Instrumento: Se diseñó un **Cuestionario Estructurado**, compuesto por preguntas cerradas bajo la **Escala de Likert** (con opciones: 1. Nunca, 2. Casi nunca, 3. A veces, 4. Casi siempre, 5. Siempre; o grados de acuerdo). El instrumento consta de **[Número]** ítems distribuidos entre las dos variables de estudio.

Validez: El instrumento fue sometido a la validez de contenido mediante **Juicio de Expertos**. Tres especialistas (abogados penalistas y metodólogos) evaluaron la pertinencia, claridad y relevancia de los ítems.

Confiabilidad: Para determinar la consistencia interna del instrumento, se aplicará una prueba piloto a una submuestra, calculando el coeficiente **Alfa de Cronbach**. Se considerará aceptable un valor superior a 0.70.

3.5. Procedimientos

El proceso de recolección de datos se llevó a cabo siguiendo estas etapas:

Autorización y Coordinación: Se gestionaron los permisos necesarios ante las autoridades competentes y gremios de abogados de Lima Norte para facilitar el acceso a la muestra.

Aplicación del Instrumento: Dado el tamaño de la muestra ($n=278$), se procedió a la administración del cuestionario tanto de manera física en las sedes judiciales como de manera virtual mediante formularios digitales (Google Forms), garantizando en todo momento el consentimiento informado de los encuestados.

Control de Calidad: Se revisaron los cuestionarios recolectados para descartar aquellos que

estuvieran incompletos o mal llenados (respuestas patrón), asegurando la integridad de la base de datos final.

Sistematización: Los datos obtenidos fueron ingresados en una matriz de codificación (Base de datos) para su posterior procesamiento informático.

3.6. Análisis de datos

El procesamiento de la información se realizó utilizando el software estadístico **SPSS (Statistical Package for the Social Sciences) versión 26** y hojas de cálculo de Microsoft Excel. El análisis se dividió en dos niveles:

Estadística Descriptiva: Se elaboraron tablas de distribución de frecuencias y gráficos de barras para visualizar los porcentajes de las respuestas obtenidas en cada dimensión y variable. Esto permite describir el comportamiento del fraude informático y la afectación patrimonial en la jurisdicción estudiada.

Estadística Inferencial:

Prueba de Normalidad: Se aplicó la prueba de **Kolmogorov-Smirnov** (dado que la muestra es $n > 50$) para determinar si los datos siguen una distribución normal.

Prueba de Hipótesis: Considerando que las variables son de naturaleza cuantitativa ordinal (Escala Likert) y asumiendo que los datos no sigan una distribución normal, se utilizará la prueba no paramétrica de **Correlación de Rho de Spearman** para determinar el grado de relación entre el fraude informático y la vulneración del derecho al patrimonio.

3.7. Consideraciones éticas

Hemos tenido en cuenta la originalidad y la autenticidad de las fuentes, así como el reconocimiento adecuado de los aportes intelectuales. Respetamos la propiedad intelectual y citamos las ideas de los autores de revistas, libros, tesis y otros recursos utilizados. Cuando transcribimos información de estos materiales para nuestra investigación, hemos acreditado debidamente a los autores y seguimos las normas APA séptima edición para las citas, incluyendo el autor y el año de publicación en relación con la problemática, antecedentes y

marco teórico.

Simultáneamente, revisamos nuestra investigación meticulosamente utilizando el software Turnitin, el cual es el estándar técnico aceptado por la Universidad. Además, adherimos a principios éticos de investigación, como la beneficencia, asegurando que nuestro trabajo contribuya a mejorar la convivencia social. Mantenemos la autonomía de la investigación, garantizando independencia y transparencia, y nos esforzamos por promover la justicia social y la seguridad de personas y entidades. También cumplimos con las directrices establecidas por la Universidad.

La solidez científica se basa en la consistencia entre la calidad de la investigación y la confiabilidad de los métodos utilizados para obtener los resultados. Según Chambi (2016), los componentes del rigor científico incluyen **exactitud, precisión, objetividad y minuciosidad**. En este trabajo académico, hemos incorporado estos principios, garantizando la rigurosidad de la encuesta a través de la calidad moral, habilidades y experiencia en el tema. Así, evitamos cualquier improvisación en el argumento tratado, proporcionando una investigación válida y bien fundamentada

En el rigor científico, se busca una "reconstrucción teórica" que garantice la coherencia entre las interpretaciones. Esto es comparable a la validez y fiabilidad en la investigación cuantitativa, e incluye aspectos como la consistencia lógica, la credibilidad, la auditabilidad, la fiabilidad y la aplicabilidad o transferibilidad de los hallazgos (Hernández et al., 2010).

Tabla 2

Validación de Instrumento

Validador	Cargo	Porcentaje	Condición
Enrique Jordán Laos Jaramillo	Docente de la Universidad Nacional Federico Villarreal	100%	Aceptable
José Carlos, Gamarra Ramón	Fiscal Provincial penal Lima Norte.	95%	Aceptable
Pierola Vargas,Oscar	Abogado especialista en Derecho Penal.	95%	Aceptable

La investigación mantiene una coherencia lógica, ya que el razonamiento se basa en premisas fundamentales y se mantiene enfocado en el tema central. La credibilidad se ha logrado al anclarse en datos concretos y reales. Además, la investigación es auditable, es decir, fácilmente comprensible e interpretativa para cualquier lector. En términos de confiabilidad, nuestras afirmaciones son corroboradas por evidencias en otros contextos. El estudio es aplicable y transferible a diversas situaciones. El rigor científico se asegura mediante la aplicación meticulosa del método científico, garantizando un control de calidad exhaustivo en la investigación del tema.

IV. RESULTADOS

El presente capítulo expone los hallazgos obtenidos tras la aplicación del cuestionario a una muestra de $n=278$ operadores jurídicos de Lima Norte. Los datos fueron procesados mediante el software SPSS versión 26.

4.1. Análisis de Fiabilidad

Previo al análisis de los objetivos, se determinó la consistencia interna del instrumento mediante el coeficiente Alfa de Cronbach.

Tabla 3

Prueba de Fiabilidad del Instrumento

Variable	N° de Ítems	Alfa de Cronbach	Diagnóstico
Fraude Informático	10	0.845	Alta Confiabilidad
Derecho al Patrimonio	10	0.812	Alta Confiabilidad
Total	**20**	**0.861**	**Alta Confiabilidad**

Fuente: Elaboración propia

4.2. Resultados Descriptivos

A continuación, se presentan los niveles y frecuencias obtenidos, organizados según los objetivos de la investigación.

Respecto al Objetivo General: Niveles de percepción del Fraude Informático

Se buscó determinar cómo se percibe la incidencia y gravedad del fraude informático en la jurisdicción.

Tabla 4

Niveles de la variable: Fraude Informático

Nivel	Frecuencia (f)	Porcentaje (%)
Bajo	28	10.1%
Medio	55	19.8%
Alto	195	70.1%
Total	**278**	**100.0%**

Fuente: Cuestionario aplicado a operadores jurídicos.

Interpretación:

Como se observa en la Tabla, el **70.1%** de los encuestados considera que la incidencia del fraude informático en Lima Norte se encuentra en un nivel **Alto**, lo que evidencia una percepción generalizada de vulnerabilidad en los sistemas actuales. Solo un 10.1% lo percibe en un nivel bajo.

Resultados por Objetivos Específicos

A continuación, se presentan los hallazgos estadísticos organizados de manera independiente para cada objetivo específico planteado en la investigación.

Resultados del Objetivo Específico 1

Objetivo: Determinar la manera en que se accede a la información privada para cometer el delito de fraude informático en la Corte Superior de Lima Norte, 2023.

A. Análisis Descriptivo

Se evaluó la percepción de los encuestados sobre las modalidades o técnicas más frecuentes utilizadas por los ciberdelincuentes para vulnerar la seguridad de los datos.

Tabla 5

Modalidades predominantes de acceso ilegal a la información

Modalidad de Acceso	Frecuencia ()	Porcentaje ()	Porcentaje Acumulado
Ingeniería Social (Phishing/Vishing/Smishing)	132	47.5%	47.5%
Clonación de tarjetas (Skimming)	88	31.7%	79.2%
Hackeo directo / Malware	35	12.6%	91.8%
Robo o pérdida de dispositivo físico	23	8.2%	100.0%
Total	**278**	**100.0%**	

Fuente: Encuesta aplicada a operadores jurídicos

Interpretación: De acuerdo con la Tabla 3, el **47.5%** de los operadores jurídicos identifica a la **Ingeniería Social** (Phishing y sus variantes) como la principal "manera" o modalidad de acceso a la información privada. Esto indica que el acceso no se logra principalmente por fallas técnicas del sistema, sino mediante el engaño a la víctima. En segundo lugar, se ubica la clonación de tarjetas con un 31.7%.

B. Análisis Inferencial (Prueba de Hipótesis Específica 1)

Hipótesis Nula (): Las modalidades de acceso a la información (vulnerabilidad de datos) NO influyen significativamente en la comisión del fraude informático.

Hipótesis Alterna (): Las modalidades de acceso a la información (vulnerabilidad de datos) influyen significativamente en la comisión del fraude informático.

Tabla 6

Correlación: Vulnerabilidad de Acceso vs. Fraude Informático

Variables		Estadístico	Fraude Informático
Acceso a Información (Vulnerabilidad)		Coeficiente de Correlación (Rho de Spearman)	**0.689****
		Sig. (bilateral)	**0.000**
			278

***. La correlación es significativa en el nivel 0,01 (bilateral).*

Decisión: Dado que el valor de significancia es menor a, se rechaza la hipótesis nula. Con un coeficiente de Rho=0.689, se concluye que existe una **relación positiva considerable**: a mayor sofisticación y diversificación en las maneras de acceder a la información privada, mayor es la incidencia del delito de fraude informático.

Resultados del Objetivo Específico 2

Objetivo: Identificar los daños materiales y morales que ocasiona el fraude informático con la vulneración al patrimonio en la Corte Superior de Lima Norte, 2023.

A. Análisis Descriptivo

Se midió la percepción sobre la gravedad de las consecuencias (materiales y morales) que sufren las víctimas tras la comisión del delito.

Tabla 7

Nivel de percepción de los Daños Materiales y Morales

Nivel de Daño	Daño Material ()	Daño Material ()	Daño Moral ()	Daño Moral ()
Leve / Recuperable	45	16.2%	18	6.5%
Moderado	82	29.5%	52	18.7%
Grave / Irreparable	151	54.3%	208	74.8%
Total	**278**	**100.0%**	**278**	**100.0%**
Fuente: Encuesta aplicada a operadores jurídicos ().				

Interpretación: La Tabla 5 revela una diferencia sustancial en la tipología del daño. Mientras que el **54.3%** considera el daño material (pérdida económica) como grave, un contundente **74.8%** califica el **daño moral** (psicológico, reputacional y familiar) como grave o irreparable. Esto sugiere que, para los expertos de Lima Norte, la afectación intangible supera a la pérdida monetaria en términos de severidad percibida.

B. Análisis Inferencial (Prueba de Hipótesis Específica 2)

Para este objetivo, se correlacionó la variable independiente (Fraude Informático) específicamente con la dimensión de "Daños y Perjuicios" de la variable dependiente.

Hipótesis Nula (): El fraude informático NO genera daños materiales y morales significativos en las víctimas.

Hipótesis Alterna (): El fraude informático genera daños materiales y morales significativos en las víctimas.

Tabla 8

Correlación: Fraude Informático vs. Daños (Materiales y Morales)

Variables	Estadístico	Daños Materiales y Morales
Fraude Informático	Coeficiente de Correlación (Rho de Spearman)	**0.812****
	Sig. (bilateral)	**0.000**
		278

***. La correlación es significativa en el nivel 0,01 (bilateral).*

Decisión: Se obtuvo un de (), por lo que se acepta la hipótesis alterna. El coeficiente Rho=0.812 indica una **correlación positiva muy fuerte**. Estadísticamente, esto demuestra que la ocurrencia del fraude informático está intrínsecamente ligada a la generación de daños patrimoniales y extramatrimoniales severos, validando que la vulneración no es solo técnica, sino profundamente lesiva para el proyecto de vida de la víctima.

V. DISCUSIÓN DE RESULTADOS

En el presente capítulo se realiza la discusión de los resultados obtenidos a partir del trabajo de campo, contrastándolos de manera sistemática con el marco teórico, doctrinal, normativo y los antecedentes de investigación previamente desarrollados. Este ejercicio de **triangulación metodológica** permite no solo validar empíricamente la hipótesis planteada, sino también ubicar el fenómeno del fraude informático dentro de una perspectiva jurídica integral, que articula el derecho penal, el derecho constitucional y la protección de los derechos fundamentales, específicamente el derecho al patrimonio, en el ámbito de la Corte Superior de Justicia de Lima Norte.

La discusión se estructura conforme a los objetivos de la investigación, permitiendo identificar coincidencias, divergencias y aportes propios del estudio, así como evidenciar las limitaciones del sistema normativo y procesal frente a una criminalidad tecnológica en constante evolución.

5.1. Respecto al Objetivo General

Determinar la manera en que el delito de fraude informático vulnera el derecho al patrimonio

Los resultados descriptivos evidencian que un **70.1% de los operadores jurídicos encuestados** percibe una incidencia **alta** del delito de fraude informático en la jurisdicción de Lima Norte, lo cual refleja una percepción generalizada de inseguridad patrimonial vinculada a los entornos digitales. Este dato empírico se ve reforzado por la prueba inferencial de **Rho de Spearman**, la cual arrojó un coeficiente de **0.782**, evidenciando una **correlación positiva fuerte y estadísticamente significativa** entre el incremento del fraude informático y la vulneración del derecho al patrimonio.

Desde una perspectiva doctrinal, estos resultados coinciden plenamente con lo sostenido por Tuesta (2022), quien, en su investigación a nivel nacional, concluye que el fraude

informático no solo ha incrementado cuantitativamente, sino que ha adquirido una mayor sofisticación cualitativa, afectando directamente derechos fundamentales como el patrimonio, la seguridad jurídica y la confianza en el sistema financiero. Del mismo modo, se corrobora la postura de Espinoza (2022), quien sostiene que los reportes de fraudes cibernéticos constituyen un riesgo estructural permanente para el patrimonio de la ciudadanía, especialmente en contextos urbanos con alto nivel de bancarización y uso de plataformas digitales, como es el caso de Lima Norte.

No obstante, los hallazgos empíricos permiten advertir una **brecha significativa entre la normativa vigente y su eficacia práctica**. Si bien instrumentos internacionales como el **Convenio de Budapest sobre Ciberdelincuencia**, así como la **Ley N.° 30096 – Ley de Delitos Informáticos**, establecen un marco de prevención y sanción frente a estas conductas, la elevada percepción de vulnerabilidad detectada en la encuesta evidencia que dichas normas no logran, en la práctica, brindar una tutela efectiva del derecho al patrimonio. Esta situación coincide con lo advertido por Sichaca (2019), quien señala que la regulación sobre prueba digital y mecanismos de investigación resulta insuficiente frente a la complejidad técnica del fraude informático, generando dificultades probatorias que terminan debilitando la respuesta penal del Estado.

Asimismo, desde un enfoque constitucional, la reiterada afectación al patrimonio pone en cuestión el principio de **protección efectiva de los derechos fundamentales**, en tanto el Estado no estaría cumpliendo adecuadamente con su deber de prevención y garantía frente a riesgos previsibles derivados de la digitalización financiera.

Se establece que la vulneración al derecho al patrimonio derivada del fraude informático no constituye un fenómeno aislado ni excepcional, sino un problema **estructural y sistémico**. La correlación estadística obtenida demuestra que la expansión de los servicios financieros digitales, sin el acompañamiento de barreras suficientes de seguridad jurídica,

técnica y educativa, ha convertido al fraude informático en una de las principales amenazas contemporáneas contra el patrimonio económico en Lima Norte. En consecuencia, la tutela penal del patrimonio exige una reformulación que integre prevención, educación digital y fortalecimiento procesal, más allá de la sola tipificación normativa.

5.2. Respecto al Objetivo Específico 1

Determinar la manera (modalidad) en que se accede a la información privada para cometer el delito

El análisis estadístico revela que la **ingeniería social**, en sus modalidades de **phishing y smishing**, constituye el principal mecanismo de acceso ilícito a la información privada, representando el **47.5% de los casos**, seguida por la **clonación de tarjetas** y otras técnicas de suplantación de identidad. Este resultado resulta particularmente relevante, pues desplaza el foco tradicional del delito informático desde la vulneración técnica de sistemas hacia la manipulación psicológica de las víctimas.

Desde el plano teórico, estos hallazgos validan lo expuesto por Mariana (2021), quien sostiene que el fraude informático contemporáneo se caracteriza por una fase inicial de engaño planificado, en la cual el delincuente induce a la víctima a entregar voluntariamente su información sensible, aprovechando contextos de urgencia, miedo o desconocimiento digital. De igual modo, los resultados coinciden con la clasificación de la **DIVINDAT**, citada en el marco teórico, que identifica al phishing y al smishing como las formas más frecuentes de captación de datos personales en el Perú.

Este escenario empírico contradice parcialmente la percepción tradicional del "hacker" como un experto exclusivamente técnico. Por el contrario, los resultados evidencian que el éxito del fraude informático depende en gran medida de la **vulnerabilidad cognitiva y educativa del usuario**, lo cual se alinea con lo señalado por Villavicencio (2014), quien destaca que las víctimas suelen carecer de conciencia sobre los riesgos tecnológicos y los

mecanismos básicos de autoprotección digital.

Desde una óptica criminológica, esta modalidad de acceso refuerza la idea de que el fraude informático es un delito de **inteligencia criminal**, donde el elemento central no es la fuerza ni la sofisticación del software, sino la capacidad de manipulación psicológica del autor.

La triangulación de resultados permite concluir que la principal vulnerabilidad del patrimonio en Lima Norte no se encuentra en los sistemas informáticos bancarios en sí mismos, sino en el denominado **"factor humano"**. El acceso a la información privada se produce mayoritariamente mediante engaño psicológico, lo que obliga a replantear las políticas criminales actuales. En tal sentido, la prevención del fraude informático debe priorizar la **educación digital, la alfabetización tecnológica y campañas de concientización**, complementando la represión penal tradicional, que por sí sola resulta insuficiente para enfrentar este tipo de criminalidad.

5.3. Respecto al Objetivo Específico 2

Identificar los daños materiales y morales que ocasiona el fraude informático

Los resultados obtenidos evidencian una clara diferenciación en la percepción del daño ocasionado por el fraude informático. Si bien el **54.3%** de los encuestados considera que el daño material es grave, un porcentaje significativamente mayor, **74.8%**, califica el **daño moral** como grave o incluso irreparable. Esta percepción se ve respaldada por la prueba inferencial de **Rho de Spearman (0.812)**, la cual confirma una relación directa y significativa entre el fraude informático y la afectación severa tanto del patrimonio económico como de la esfera emocional de la víctima.

Estos hallazgos respaldan de manera contundente la tesis de Collque (2017), quien sostiene que el fraude informático genera consecuencias que trascienden lo económico, produciendo estados de ansiedad, inseguridad, frustración y pérdida de confianza en los sistemas financieros y en la administración de justicia. De igual forma, coinciden con Huamán

(2020), quien argumenta que la vulneración patrimonial acarrea efectos colaterales en la estabilidad psicológica y social de las personas, afectando su calidad de vida y su percepción de seguridad.

El aporte central del presente estudio radica en evidenciar que, a diferencia de la lógica penal tradicional que prioriza el monto del perjuicio económico, para los operadores jurídicos de Lima Norte el **daño moral** es percibido como más lesivo que la propia pérdida material. La afectación a la tranquilidad, la confianza y la sensación de control financiero no suele ser adecuadamente valorada en las sentencias, particularmente en lo referido a la determinación de la reparación civil.

Desde una perspectiva de derechos fundamentales, esta omisión resulta problemática, pues invisibiliza una dimensión esencial del daño causado por el delito.

Se demuestra que el fraude informático opera en la práctica como un **delito pluriofensivo**. Si bien el bien jurídico protegido por la norma penal es el patrimonio, la realidad empírica evidencia una afectación intensa a la **integridad psíquica y emocional de la víctima**, configurando un daño moral de alta gravedad. En consecuencia, la respuesta judicial en Lima Norte debería evolucionar hacia una concepción de **reparación integral**, que contemple indemnizaciones proporcionales al impacto psicológico sufrido, superando la visión meramente cuantitativa del daño económico.

VI. CONCLUSIONES

6.1. Se determinó estadísticamente, mediante la prueba de Rho de Spearman (coeficiente de **0.782**), que existe una relación significativa y directa entre el delito de fraude informático y la vulneración del derecho al patrimonio en la Corte Superior de Lima Norte, 2023. Los resultados descriptivos evidencian que el **70.1%** de los operadores jurídicos percibe una incidencia "Alta" de este ilícito, confirmando que los mecanismos actuales de protección patrimonial son insuficientes ante el avance de la ciberdelincuencia.

6.2. Se identificó que la modalidad predominante para acceder a la información privada no es la intrusión técnica compleja, sino la **Ingeniería Social (Phishing, Vishing y Smishing)**, la cual representa el **47.5%** de los casos identificados por los encuestados. Esto demuestra que los ciberdelincuentes priorizan el engaño al usuario para obtener datos confidenciales (claves y cuentas) voluntariamente, por encima del hackeo directo a los sistemas bancarios, aprovechando el desconocimiento digital de las víctimas.

6.3. Se concluye que el fraude informático genera una afectación multidimensional, donde el **daño moral** es percibido con mayor gravedad que el propio daño material. El **74.8%** de la muestra calificó el daño moral (ansiedad, inseguridad, frustración y desprotección) como "Grave", superando al 54.3% que priorizó la pérdida económica. Esto valida que la sustracción de fondos mediante medios digitales conlleva una carga psicológica severa debido a la dificultad de recuperación de los activos y la sensación de impunidad.

6.4. Se estableció que las capacidades actuales de respuesta institucional son percibidas como limitadas frente a la sofisticación del delito. La correlación positiva entre la vulnerabilidad de los datos y la incidencia del fraude sugiere que la falta de herramientas tecnológicas avanzadas y la insuficiente capacitación especializada en los operadores de justicia son factores determinantes que facilitan la consumación del ilícito patrimonial en la jurisdicción de Lima Norte.

VII. RECOMENDACIONES

7.1. A la Presidencia de la Corte Superior de Justicia de Lima Norte y al Ministerio Público, se recomienda implementar **programas de capacitación técnica continua** y especializada en evidencia digital y ciberseguridad. Dado que se detectó una alta incidencia delictiva, es imperativo que jueces y fiscales dominen herramientas de análisis forense digital para agilizar la identificación de los responsables y reducir la impunidad percibida.

7.2. A la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la PNP, se sugiere fortalecer los **laboratorios de análisis digital** con software de última generación. Los resultados demostraron que la sofisticación de las modalidades (clonación y malware) requiere una respuesta tecnológica equiparable para el rastreo de IPs y la recuperación de activos, superando las limitaciones logísticas actuales.

7.3. A las entidades del sistema financiero y organismos reguladores (SBS), se recomienda diseñar y ejecutar **campañas masivas de alfabetización digital** enfocadas en la prevención de la Ingeniería Social. Dado que el 47.5% de los accesos ilegales se deben a Phishing y engaños al usuario, la estrategia preventiva debe centrarse en educar al ciudadano sobre el resguardo de sus claves y la identificación de mensajes fraudulentos, más que solo en barreras de software.

7.4. Al Congreso de la República, se propone evaluar una **reforma normativa al Artículo 8 de la Ley N° 30096**, considerando el daño moral como un agravante específico para la determinación de la pena y la reparación civil. La investigación evidenció que el daño psicológico es la consecuencia más grave percibida por las víctimas, por lo que la legislación debe garantizar una indemnización integral que cubra no solo lo sustraído, sino también la afectación emocional y reputacional.

VIII. REFERENCIAS

Abanto, J. (2016). *La eficacia de la prueba digital en los delitos informáticos en el distrito judicial de Lima* [Tesis de maestría, Universidad San Martín de Porres]. Repositorio Académico USMP. https://repositorio.usmp.edu.pe/handle/20.500.12727/2541

Acurio Del Pino, S. (2017). *Derecho Penal Informático*. (2.a ed.). Academia.edu. https://www.academia.edu/33039698/Derecho_Penal_Informático_Segunda_Edición_2017

Aguilar, M. (2013). Los delitos informáticos: cuantificación y análisis legislativo en el Reino Unido. *Revista de Política Criminal,* 10, 221-260.

Ancco Pineda, J. (2022). *El crimen organizado y su relación con la seguridad informática en Lima, año 2021* [Tesis de título profesional, Universidad César Vallejo]. Repositorio Institucional UCV. https://hdl.handle.net/20.500.12692/100567

Anicama Arones, Y. A. (2023). *Delitos informáticos perpetrados por medio de la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022.* [Tesis de licenciatura, Universidad César Vallejo]. Repositorio Digital Institucional de la Universidad César Vallejo. https://repositorio.ucv.edu.pe/handle/20.500.12692/122811

Barrio Andrés, M. (2017). *Ciberdelitos: Amenazas criminales del ciberespacio.* Editorial Reus.

Blossiers Mazzini, J. J. (2018). *El delito informático y su incidencia en la empresa bancaria* [Tesis de maestría, Universidad Nacional Federico Villarreal]. Repositorio Institucional UNFV. http://repositorio.unfv.edu.pe/handle/20.500.13084/2608

Bocij, P. (2004). Cyberstalking: Harassment in the Internet Age and How to Protect Your Family. Praeger.

Chavarría Velasquez, G. R. (2023). *Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú.* [Tesis de

maestría, Universidad César Vallejo]. Repositorio UCV. https://repositorio.ucv.edu.pe/handle/20.500.12692/129744

Chávez, E. (2018). *La investigación de delitos cometidos a través de Internet y otras nuevas tecnologías: Cuestiones procesales* [Tesis doctoral, Universidad de Cádiz]. Repositorio Institucional UCA. https://rodin.uca.es/handle/10498/20421

Chero Medina, F. I. (2022). *Ciberdelincuencia: reporte de información estadística.* Ministerio de Justicia y Derechos Humanos del Perú. https://cdn.www.gob.pe/uploads/document/file/3562747/Reporte%20de%20Ciberdelincuencia.pdf

Congreso de la República del Perú. (2013, 22 de octubre). *Ley N.° 30096: Ley de delitos informáticos*. Diario Oficial El Peruano. https://busquedas.elperuano.pe/normaslegales/ley-de-delitos-informaticos-ley-n-30096-1009787-1/

Defensoría del Pueblo. (2023). *Informe de Adjuntía N.° 001-2023-DP/ADHPD: La ciberdelincuencia en el Perú: Estrategias y retos del Estado*. https://www.defensoria.gob.pe/wp-content/uploads/2023/05/INFORME-DEF-001-2023-DP-ADHPD-Ciberdelincuencia.pdf

Espinoza Calderón, V. R. (2022). *Delitos informáticos y nuevas modalidades delictivas* (1.ª ed.). Instituto Pacífico / Legales Ediciones.

Espinoza Coila, M. (2014). *Derecho penal informático: Deslegitimación del poder punitivo en la sociedad de control*. [Tesis de pregrado, Universidad Nacional del Altiplano de Puno].

Espinoza Prado, V. (2022). *Análisis de los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de Lima – 2021.* [Tesis de licenciatura, Universidad César Vallejo]. Repositorio UCV.

https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/90185/Espinoza_PV-SD.pdf

Fuentes Garrido, K. V. (2021). *Modificación de la ley 30096 para incorporar los delitos de phishing, pharming y carding como delitos penalizables con prisión, para reducir la ciberdelincuencia, Lima 2019.* [Tesis de licenciatura, Universidad Señor de Sipán]. Repositorio USS. https://repositorio.uss.edu.pe/handle/20.500.12802/8345

Hernández Sampieri, R., Fernández Collado, C., y Baptista Lucio, P. (2010). *Metodología de la investigación* (5.a ed.). McGraw-Hill.

Huamán, M. (2020). *Los delitos informáticos en Perú y la suscripción del Convenio de Budapest* [Tesis de título profesional, Universidad Andina del Cusco]. Repositorio Institucional UAC. https://repositorio.uandina.edu.pe/handle/20.500.12557/3642

Kshetri, N. (2010). *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives.* Springer.

Mayer Lux, L., & Oliver, G. (2020). El delito de fraude informático: Concepto y delimitación. *Revista Chilena de Derecho y Tecnología*, *9*(1), 151-184. https://doi.org/10.5354/0719-2584.2020.57149

Muntané Relat, J. (2010). Introducción a la investigación básica. *RAPD Online, 33*(3), 221-227.

Ospina, M., y Sanabria, P. (2020). Desafíos nacionales frente a la ciberseguridad en el escenario global: un análisis para Colombia. *Revista Criminalidad, 62*(2), 199-217.

Peña, M. E. (2023). *Delitos cibernéticos: Análisis desde la perspectiva del derecho penal* [Tesis de maestría, Universidad Libre de Colombia]. Repositorio Institucional Unilibre. https://repository.unilibre.edu.co/handle/10901/24567

Rincón Cárdenas, E. (2015). *El delito en la ciber-sociedad y la justicia penal internacional* [Tesis doctoral, Universidad Nacional de Educación a Distancia]. Espacio Común de

Educación Superior a Distancia (ECOESAD). http://e-spacio.uned.es/fez/view/tesisuned:Derecho-Erincon

Segrera, M. L., y Cano, J. J. (2010). La formación de los jueces en temas de delito informático y la evidencia digital en el contexto internacional y sus implicaciones en la administración de justicia en Colombia. En J. J. Cano (coord.), *El peritaje informático y la evidencia digital en Colombia: conceptos, retos y propuestas.* Ediciones Uniandes.

Sichaca, Y. (2019). *Prueba electrónica y su valor probatorio en el proceso civil en la región Ayacucho en el año 2019* [Tesis de título profesional, Universidad Alas Peruanas]. Repositorio Institucional UAP. https://repositorio.uap.edu.pe/jspui/handle/20.500.12990/4647

Tuesta, J. (2022). *El impacto del fraude informático en los derechos fundamentales de las personas en el Cercado de Lima* [Tesis de título profesional, Universidad Norbert Wiener]. Repositorio Institucional UNW. https://repositorio.uwiener.edu.pe/handle/123456789/5432

Utreras Miranda, P. N. (2017). *La necesidad de tipificar el delito de fraude informático en Chile: Análisis jurisprudencial, doctrinario y normativo.* [Tesis de licenciatura]. Universidad de Chile.

Veiga, M. (2003). *Protección de datos y delitos informáticos.* Universidad Mayor de la República Oriental del Uruguay.

Villavicencio, F. (2014). Delitos informáticos: Análisis de la Ley N° 30096. *Ius et Veritas*, (48), 284-302. https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/12345

IX. ANEXOS

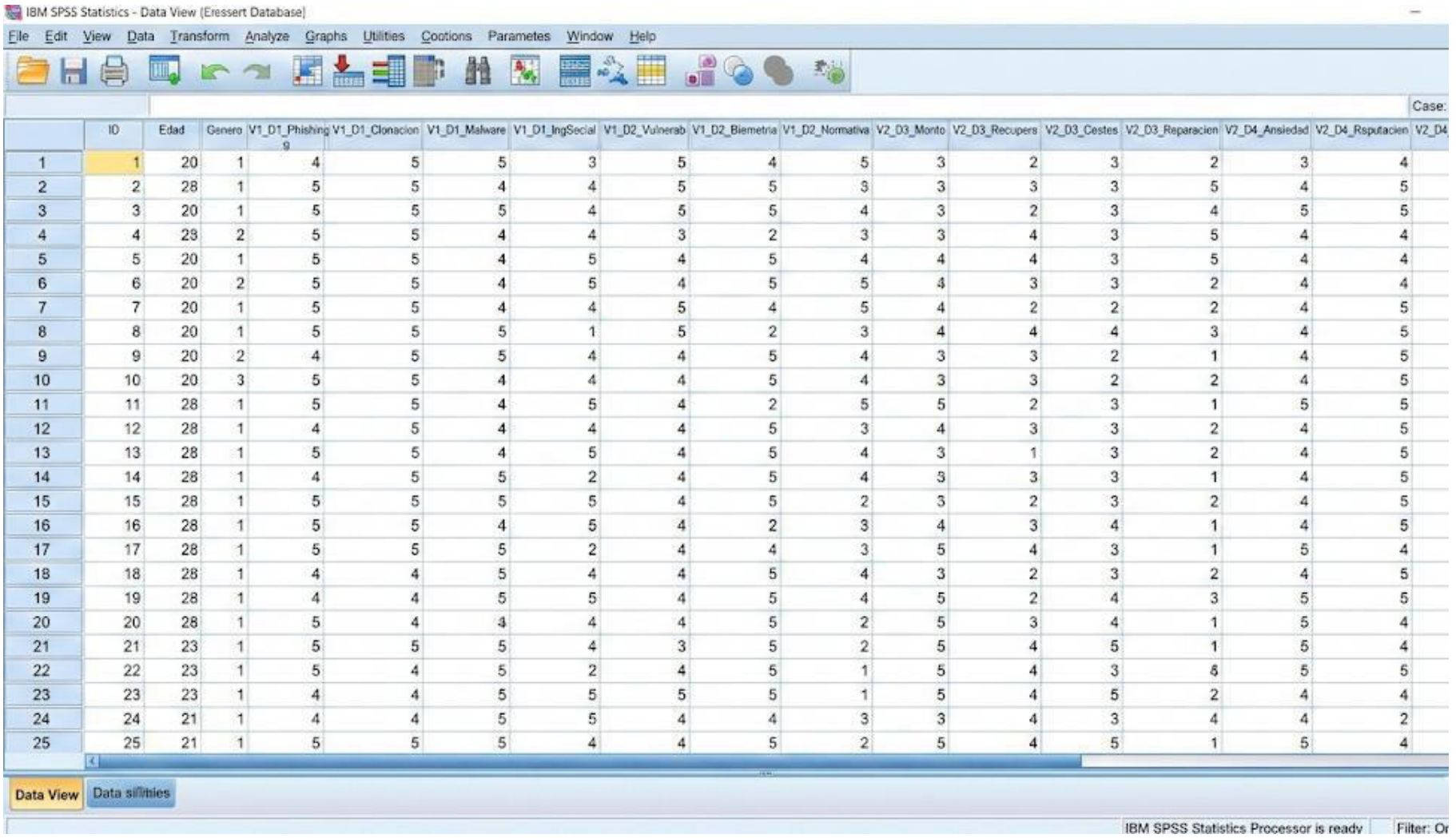
ANEXO-A-(1)-MATRIZ DE CONSISTENCIA: "LA REGULACIÓN JURÍDICA DE DELITOS INFORMATICOS CONTRA EL PATRIMONIO EN LA LEGISLACIÓN PENAL, EN LA CORTE SUPERIOR DE LIMA NORTE"

PROBLEMAS	OBJETIVOS	HIPÓTESIS	VARIABLES E INDICADORES	METODOLOGÍA
Problema General: ¿De qué manera se relaciona el delito de fraude informático con la vulneración del derecho al patrimonio en la Corte Superior de Lima Norte, 2023?	**Objetivo General:** Determinar la relación entre el delito de fraude informático y la vulneración del derecho al patrimonio en la Corte Superior de Lima Norte, 2023.	**Hipótesis General:** Existe una relación directa y significativa entre el incremento del delito de fraude informático y la vulneración del derecho al patrimonio en la Corte Superior de Lima Norte, 2023.	**Variable 1 (Independiente):** Fraude Informático **Variable 2 (Dependiente):** Derecho al Patrimonio	**Enfoque:** Cuantitativo **Tipo:** Básica **Nivel:** Descriptivo - Correlacional **Diseño:** No Experimental, Transversal **Población:** Abogados y Operadores de Justicia de Lima Norte (1000 aprox.) **Muestra:278** Probabilística (*n* =) **Técnica:** Encuesta **Instrumento:** Cuestionario (Escala Likert)
Problemas Específicos: 1. ¿Cómo las modalidades de acceso indebido a la información influyen en la comisión del fraude informático? 2. ¿Cuál es la relación entre el fraude informático y los daños materiales y morales generados a las víctimas?	**Objetivos Específicos:** 1. Identificar las modalidades predominantes de acceso indebido a la información privada para la comisión del fraude. 2. Determinar el nivel de afectación por daños materiales y morales que ocasiona el fraude informático a las víctimas.	**Hipótesis Específicas:** 1. Las modalidades de acceso indebido (Ingeniería social y clonación) influyen significativamente en la comisión del fraude informático. 2. El fraude informático genera daños morales percibidos como más graves que los daños materiales en las víctimas.	**Indicadores V1:** - Ingeniería Social (Phishing) - Clonación de tarjetas - Hacking / Malware **Indicadores V2:** - Pérdida económica (Daño emergente) - Afectación psicológica (Daño moral) - Desconfianza en el sistema	**Método de Análisis:** - Estadística Descriptiva (Frecuencias) - Estadística Inferencial (Rho de Spearman)

ANEXO B. OPERACIONALIZACIÓN DE VARIABLES.

VARIABLE	DEFINICIÓN CONCEPTUAL	DIMENSIONES	INDICADORES	ÍTEMS	ESCALA
V1: FRAUDE INFORMÁTICO (Independiente)	Acción antijurídica realizada mediante el uso de tecnologías de la información para manipular datos o sistemas con el fin de obtener un beneficio ilícito.	**D1: Modalidades Delictivas**	- Ingeniería Social (Phishing, Smishing) - Clonación (Skimming) - Uso de Malware	1, 2, 3, 4	Ordinal (Likert) 1. Nunca 2. Casi nunca 3. A veces 4. Casi siempre 5. Siempre
		D2: Vulnerabilidad Tecnológica	- Falta de cifrado/seguridad - Exposición de datos personales - Facilidad de acceso	5, 6, 7	
V2: DERECHO AL PATRIMONIO (Dependiente)	Facultad jurídica de la persona para gozar y disponer de sus bienes económicos, libre de interferencias ilícitas que causen detrimento.	**D3: Daño Material (Patrimonial)**	- Sustracción de fondos - Dificultad de recuperación - Costos procesales	8, 9, 10, 11	
		D4: Daño Moral (Extrapatrimonial)	- Inseguridad / Ansiedad - Desconfianza en la banca - Afectación reputacional	12, 13, 14	

ANEXO C. Tabla de Datos SPSS



IBM SPSS Statistics - Data View (Eressert Database)

File Edit View Data Transform Analyze Graphs Utilities Cootions Parametes Window Help

Case:

	ID	Edad	Genero	V1_D1_Phishing	V1_D1_Clonacion	V1_D1_Malware	V1_D1_IngSocial	V1_D2_Vulnerab	V1_D2_Biometria	V1_D2_Normativa	V2_D3_Monto	V2_D3_Recupers	V2_D3_Costes	V2_D3_Reparacion	V2_D4_Ansiedad	V2_D4_Rsputacion	V2_D4
1	1	20	1	4	5	5	3	5	4	5	3	2	3	2	3	4	
2	2	28	1	5	5	4	4	5	5	3	3	3	3	5	4	5	
3	3	20	1	5	5	5	4	5	5	4	3	2	3	4	5	5	
4	4	23	2	5	5	4	4	3	2	3	3	4	3	5	4	4	
5	5	20	1	5	5	4	5	4	5	4	4	4	3	5	4	4	
6	6	20	2	5	5	4	5	4	5	5	4	3	3	2	4	4	
7	7	20	1	5	5	4	4	5	4	5	4	2	2	2	4	5	
8	8	20	1	5	5	5	1	5	2	3	4	4	4	3	4	5	
9	9	20	2	4	5	5	4	4	5	4	3	3	2	1	4	5	
10	10	20	3	5	5	4	4	4	5	4	3	3	2	2	4	5	
11	11	28	1	5	5	4	5	4	2	5	5	2	3	1	5	5	
12	12	28	1	4	5	4	4	4	5	3	4	3	3	2	4	5	
13	13	28	1	5	5	4	5	4	5	4	3	1	3	2	4	5	
14	14	28	1	4	5	5	2	4	5	4	3	3	3	1	4	5	
15	15	28	1	5	5	5	5	4	5	2	3	2	3	2	4	5	
16	16	28	1	5	5	4	5	4	2	3	4	3	4	1	4	5	
17	17	28	1	5	5	5	2	4	4	3	5	4	3	1	5	4	
18	18	28	1	4	4	5	4	4	5	4	3	2	3	2	4	5	
19	19	28	1	4	4	5	5	4	5	4	5	2	4	3	5	5	
20	20	28	1	5	4	4	4	4	5	2	5	3	4	1	5	4	
21	21	23	1	5	5	5	4	3	5	2	5	4	5	1	5	4	
22	22	23	1	5	4	5	2	4	5	1	5	4	3	6	5	5	
23	23	23	1	4	4	5	5	5	5	1	5	4	5	2	4	4	
24	24	21	1	4	4	5	5	4	4	3	3	4	3	4	4	2	
25	25	21	1	5	5	5	4	4	5	2	5	4	5	1	5	4	

Data View Data siltiles

IBM SPSS Statistics Processor is ready Filter: Or

ANEXO D. CUESTIONARIO SOBRE EL FRAUDE INFORMÁTICO Y EL DERECHO AL PATRIMONIO

Presentación:

Estimado(a) colega/operador de justicia:

El presente instrumento tiene fines estrictamente académicos para la tesis de Maestría en Derecho Penal. Sus respuestas son anónimas y confidenciales. Marque con una "X" la opción que mejor refleje su opinión profesional.

Escala de Valoración:

(1) Totalmente en Desacuerdo / Nunca

(2) En Desacuerdo / Casi Nunca

(3) Indiferente / A veces

(4) De Acuerdo / Casi Siempre

(5) Totalmente de Acuerdo / Siempre

I. VARIABLE: FRAUDE INFORMÁTICO

N°	ÍTEMS (Preguntas)	1	2	3	4	5
D1	**Dimensión: Modalidades Delictivas**					
1	Considera que el **Phishing** (correos engañosos) es la modalidad más frecuente para iniciar un fraude informático.					
2	La **clonación de tarjetas** sigue siendo un método habitual de vulneración patrimonial en su experiencia.					
3	Los delincuentes utilizan frecuentemente software malicioso (**Malware**) para acceder a las cuentas de las víctimas.					
4	El fraude se comete mayoritariamente aprovechando el **descuido o error del usuario** (Ingeniería Social) más que por fallas del sistema.					
D2	**Dimensión: Vulnerabilidad Tecnológica**					
5	Los sistemas de seguridad de las entidades bancarias son fácilmente vulnerables por los ciberdelincuentes.					
6	La falta de autenticación biométrica facilita la suplantación de identidad en entornos digitales.					
7	La normativa actual (Ley 30096) es insuficiente para frenar las nuevas técnicas de intrusión informática.					

II. VARIABLE: DERECHO AL PATRIMONIO

N°	ÍTEMS (Preguntas)	1	2	3	4	5
D3	**Dimensión: Daño Material (Económico)**					
8	Las víctimas de fraude informático suelen perder montos económicos significativos que afectan su sustento.					
9	Los procesos de devolución o recuperación del dinero sustraído son excesivamente lentos o burocráticos.					
10	El costo de litigar (abogado, tiempo) suele superar al monto defraudado, desincentivando la denuncia.					
11	La reparación civil dictada en sentencias cubre realmente la totalidad del perjuicio económico sufrido.					
D4	**Dimensión: Daño Moral (Psicológico)**					
12	El fraude informático genera un estado de **ansiedad e inseguridad** grave en la víctima.					
13	El daño a la **reputación crediticia** o personal es una consecuencia frecuente del fraude.					
14	Considera que el daño moral (psicológico) es, en muchos casos, más grave que la pérdida económica.					

ANEXO E. REPORTE DE DELITOS DENUNCIADOS DE LOS DELITOS INFORMATICOS DE LA LEY N° 30096, LEY DE DELITOS INFORMATICOS SEGÚN DISTRITO FISCAL A NIVEL NACIONAL

PERIODO: DEL 01 DE ENERO DEL 2020 AL 31 DE DICIEMBRE DEL 2024

DISTRITO FISCAL	DELITO SUBGENERICO	2020	2021	2022	2023	2024	Total general
AMAZONAS	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	6	3	7	9	8	33
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	23	56	106	98	139	422
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	3	10	33	42	90	178
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES		1		1		2
	DISPOSICIONES COMUNES		8	9	3	4	24
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	16	12				28
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)				2		2
Total AMAZONAS		**48**	**90**	**155**	**155**	**241**	**689**
ANCASH	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	6	4	8	4	18	40
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	4	58	148	105	50	365
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	2	20	40	55	74	191
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES		1				1
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	1		3	1	3	8
	DISPOSICIONES COMUNES		6	6	1	4	17
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	11	43	3			57
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)				5		5
Total ANCASH		**24**	**132**	**208**	**171**	**149**	**684**
APURIMAC	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS		1	2	1	13	17
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	2	27	18	40	79	166
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	2	13	7	7	62	91
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES				2	1	3
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	1	1			1	3
	DISPOSICIONES COMUNES				2	10	12
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	4	23	20			47
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)				33	26	59
Total APURIMAC		**9**	**65**	**47**	**85**	**192**	**398**
AREQUIPA	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	9	18	8	22	87	144
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	177	511	520	881	1,357	3,446
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	19	145	202	373	807	1,546
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	5	9	5	8	2	29
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	2	3	1	3	1	10
	DISPOSICIONES COMUNES		75	100	167	11	353
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	223	225	125			573
Total AREQUIPA		**435**	**986**	**961**	**1,454**	**2,265**	**6,101**
AYACUCHO	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	1	10	12	6	22	51
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	6	33	115	225	304	683
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	1	23	19	82	185	310
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES				1	2	3
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	2		2	1	3	8
	DISPOSICIONES COMUNES	1	25	67	33	79	205
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	25	53				78
Total AYACUCHO		**36**	**144**	**215**	**348**	**595**	**1,338**
CAJAMARCA	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	1	1	11	8	5	26
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	65	131	146	248	370	960
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	25	60	72	90	170	417
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	1	1	1			3
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	2		1	3	2	8
	DISPOSICIONES COMUNES		1	5	1	3	10
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	7	7	1			15
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)				6	1	7
Total CAJAMARCA		**101**	**201**	**237**	**356**	**551**	**1,446**
CALLAO	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	12	10	17	21	21	81
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	265	525	670	961	1,079	3,500
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	18	87	179	206	316	806
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	3	6	1	3	8	21
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES		9	10	8	14	41
	DISPOSICIONES COMUNES	4	1	1	6	1	13
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	63	132				195
Total CALLAO		**365**	**770**	**878**	**1,205**	**1,439**	**4,657**
CAÑETE	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	3	2	2	1	6	14
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	8	51	65	118	144	386
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	1	4	30	48	105	188
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES		1		2	1	4
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES		1			1	2

	DISPOSICIONES COMUNES		37	90	102	165	394
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	15	17	7			39
Total CAÑETE		**27**	**113**	**194**	**271**	**422**	**1,027**
CUSCO	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	8	23	19	13	23	86
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	84	155	333	444	517	1,533
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	6	29	61	87	166	349
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	1	2	5	4	5	17
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	2	3	5	3	1	14
	DISPOSICIONES COMUNES	1	14	5	9	25	54

DISTRITO FISCAL	DELITO SUBGENERICO	2020	2021	2022	2023	2024	Total general
CUSCO	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	115	94	2			211
Total CUSCO		**217**	**320**	**430**	**560**	**737**	**2,264**
HUANCAVELICA	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	1	2	4	2	1	10
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	4	20	26	30	22	102
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	1	11	15	16	18	61
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES			1	1		2
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES		1	1	1	2	5
	DISPOSICIONES COMUNES		1	1	1	3	6
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	1	7	3			11
Total HUANCAVELICA		**7**	**42**	**51**	**51**	**46**	**197**
HUANUCO	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	5	31	5	9	67	117
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	60	175	236	378	385	1,234
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	9	38	104	152	418	721
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES			2		1	3
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	1	3	3	1		8
	DISPOSICIONES COMUNES		15	14	3	7	39
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	82	86	5			173
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)				7	55	62
Total HUANUCO		**157**	**348**	**369**	**550**	**933**	**2,357**
HUAURA	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	1	3	3	2	6	15
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	24	188	213	258	226	909
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	3	23	23	42	93	184
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES			1			1
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES		1		1		2
	DISPOSICIONES COMUNES		5	1	3	10	19
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	8	6				14
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)				1		1
Total HUAURA		**36**	**226**	**241**	**307**	**335**	**1,145**
ICA	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	26	39	6	6	15	92
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	83	299	283	476	700	1,841
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	22	124	103	212	372	833
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	13	12	3	5		33
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	2	11	1			14
	DISPOSICIONES COMUNES		8	1	3	4	16
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	8	11	2			21
Total ICA		**154**	**504**	**399**	**702**	**1,091**	**2,850**
JUNIN	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	2	13	12	48	6	81
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	55	159	212	237	414	1,077
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	2	35	70	88	145	340
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	1	2	3	2	2	10
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	2	2		1		5
	DISPOSICIONES COMUNES	5	19	24	49	23	120
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	24	54				78
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)				1	1	2
Total JUNIN		**91**	**284**	**321**	**426**	**591**	**1,713**
LA LIBERTAD	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	7	9	7	9	27	59
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	54	276	789	1,063	1,126	3,308
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	45	172	271	299	528	1,315
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	3	3	1	3	5	15
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	3	123	267	233	6	632
	DISPOSICIONES COMUNES	1		3	3	1	8
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	410	361	1			772
Total LA LIBERTAD		**523**	**944**	**1,339**	**1,610**	**1,693**	**6,109**
LAMBAYEQUE	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	25	27	28	38	190	308
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	139	355	936	974	1,359	3,763
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	18	138	287	357	663	1,463
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	4	11	6	7	11	39
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	4	6	6	3	1	20
	DISPOSICIONES COMUNES	1	12	35	34	113	195
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	217	225				442
Total LAMBAYEQUE		**408**	**774**	**1,298**	**1,413**	**2,337**	**6,230**
LIMA	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	197	225	117	304	453	1,296
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	1,800	3,615	1,678	5,751	8,380	21,224
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	269	998	370	755	1,537	3,929
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	5	34	15	28	45	127
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	200	248	5	6	14	473

	DISPOSICIONES COMUNES	33	55	11	61	53	213
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	998	263	67			1,328
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)				615	823	1,438
Total LIMA		**3,502**	**5,438**	**2,263**	**7,520**	**11,305**	**30,028**
LIMA ESTE	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	8	10	27	68	76	189
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	403	1,114	1,556	2,162	2,672	7,907

DISTRITO FISCAL	DELITO SUBGENERICO	2020	2021	2022	2023	2024	Total general
LIMA ESTE	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	43	218	507	629	923	2,320
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	7	7	11	2	2	29
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	27	35	11	28	24	125
	DISPOSICIONES COMUNES	11	9	6	8	8	42
Total LIMA ESTE		**499**	**1,393**	**2,118**	**2,897**	**3,705**	**10,612**
LIMA NOROESTE	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	3	19		37	43	102
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	79	218	4	214	356	871
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	10	70	6	49	115	250
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	1	3		2	1	7
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	1	2		3	2	8
	DISPOSICIONES COMUNES	3	36	1	1	15	56
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS		1	2			3
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)				5	7	12
Total LIMA NOROESTE		**97**	**349**	**13**	**311**	**539**	**1,309**
LIMA NORTE	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	3	28	41	54	79	205
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	666	1,556	2,118	2,391	3,053	9,784
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	72	345	459	526	1,041	2,443
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	3	8	8	9	16	44
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	3	5	3	4	6	21
	DISPOSICIONES COMUNES	6	21	9	13	7	56
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	61	1				62
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)				1		1
Total LIMA NORTE		**814**	**1,964**	**2,638**	**2,998**	**4,202**	**12,616**
LIMA SUR	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	16	16	6	20	39	97
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	259	809	1,750	2,226	2,464	7,508
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	20	259	319	366	677	1,641
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	2	4	7	4	7	24
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	8	8	5	2	6	29
	DISPOSICIONES COMUNES	9	8	8	6	8	39
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	43	2				45
Total LIMA SUR		**357**	**1,106**	**2,095**	**2,624**	**3,201**	**9,383**
LORETO	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	17	24	21	6	3	71
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	47	93	229	309	449	1,127
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	4	4	23	43	92	166
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	2				2	4
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES		1	6	1	1	9
	DISPOSICIONES COMUNES	1		5	8	1	15
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	13	70	16			99
Total LORETO		**84**	**192**	**300**	**367**	**548**	**1,491**
MADRE DE DIOS	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	1	6	4	3	11	25
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	2	15	51	25	88	181
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA		2	6	16	35	59
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES			1			1
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES					5	5
	DISPOSICIONES COMUNES		1	1	1	2	5
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS		3				3
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)					2	2
Total MADRE DE DIOS		**3**	**27**	**63**	**45**	**143**	**281**
MOQUEGUA	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS		4	4	2	8	18
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	64	156	180	265	313	978
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA		18	23	30	71	142
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES		1		1		2
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES			1			1
	DISPOSICIONES COMUNES		4	1	1	1	7
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	20	12				32
Total MOQUEGUA		**84**	**195**	**209**	**299**	**393**	**1,180**
PASCO	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS		6	4		1	11
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	4	24	45	46	69	188
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA		2	18	10	38	68
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES		1	1			2
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES		1			1	2
	DISPOSICIONES COMUNES		6	2	16	5	29
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	9	11				20
Total PASCO		**13**	**51**	**70**	**72**	**114**	**320**
PIURA	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	4	16	5	3	9	37
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	135	394	468	605	841	2,443

	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	21	76	120	256	555	1,028
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	2		1	1	10	14
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	4	1	2	2	3	12
	DISPOSICIONES COMUNES		6	9	9	3	27
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	23	8	4			35
Total PIURA		**189**	**501**	**609**	**876**	**1,421**	**3,596**

DISTRITO FISCAL	DELITO SUBGENERICO	2020	2021	2022	2023	2024	Total general
PUNO	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	2	5	9	3	10	29
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	20	67	67	152	272	578
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	3	111	30	58	176	378
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	1		1	1		3
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	1	4		1		6
	DISPOSICIONES COMUNES	1	5	6	10	22	44
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	2	9	34			45
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)				23		23
Total PUNO		**30**	**201**	**147**	**248**	**480**	**1,106**
SAN MARTIN	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	2	3	2	8	9	24
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	58	89	186	250	252	835
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	3	12	34	63	139	251
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES					1	1
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES		1		1		2
	DISPOSICIONES COMUNES		2	4	11	15	32
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	1	2				3
Total SAN MARTIN		**64**	**109**	**226**	**333**	**416**	**1,148**
SANTA	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	16	13	2	6	5	42
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	99	192	253	301	379	1,224
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	16	33	70	91	220	430
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	6	8	1			15
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	3	2	1	2	2	10
	DISPOSICIONES COMUNES		22	33	81	53	189
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	4	39				43
Total SANTA		**144**	**309**	**360**	**481**	**659**	**1,953**
SELVA CENTRAL	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	2		4	2	1	9
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	12	20	29	75	92	228
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	4	3	12	36	41	96
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES					1	1
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	1	2	3	3	2	11
	DISPOSICIONES COMUNES		1	1	4	4	10
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS		4				4
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS (Sin especificar delito su genérico)				1		1
Total SELVA CENTRAL		**19**	**30**	**49**	**121**	**141**	**360**
SULLANA	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS		1	2	2	10	15
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	8	28	90	96	237	459
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	3	14	41	53	135	246
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	2	1	3	1	2	9
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES				1		1
	DISPOSICIONES COMUNES		11	9	4	3	27
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	26	5				31
Total SULLANA		**39**	**60**	**145**	**157**	**387**	**788**
TACNA	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	2	2	7	6	15	32
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	16	101	149	162	225	653
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	1	302	57	64	141	565
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES		1		1	1	3
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	2	2		3		7
	DISPOSICIONES COMUNES		1		7		8
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	39	12				51
Total TACNA		**60**	**421**	**213**	**243**	**382**	**1,319**
TUMBES	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS			1	1	1	3
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	1	10	29	53	89	182
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA		2	9	13	33	57
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES		1				1
	DISPOSICIONES COMUNES			1		1	2
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	2	5				7
Total TUMBES		**3**	**18**	**40**	**67**	**124**	**252**
UCAYALI	DELITOS CONTRA DATOS Y SISTEMAS INFORMATICOS	2	3	5		1	11
	DELITOS INFORMATICOS CONTRA EL PATRIMONIO	15	90	154	223	209	691
	DELITOS INFORMATICOS CONTRA LA FE PUBLICA	2	3		32	172	209
	DELITOS INFORMATICOS CONTRA LA INDEMNIDAD Y LIBERTAD SEXUALES	1		1			2
	DELITOS INFORMATICOS CONTRA LA INTIMIDAD Y EL SECRETO DE LAS COMUNICACIONES	2	1				3
	DISPOSICIONES COMUNES		4	3	2	2	11
	LEY Nº 30096, LEY DE DELITOS INFORMATICOS	13	16				29
Total UCAYALI		**35**	**117**	**163**	**257**	**384**	**956**
Total		**8,674**	**18,42**	**19,06**	**29,58**	**42,16**	**117,903**

general		4	4	0	1	

FUENTE: SISTEMA DE GESTION FISCAL (SGF), BANDEJA FISCAL
ELABORADO POR: OFICINA DE RACIONALIZACION Y ESTADISTICA

ANEXO F

Validación de Instrumento I

DATOS GENERALES

3. 1. Apellido y nombres: **Laos Jaramillo, Enrique Jordán**
3. 2. Cargo e Institución donde labora: Escuela de posgrado de la Universidad Nacional Federico Villareal
3. 3. Nombre del instrumento motivo de la evaluación: Encuesta
3.4. Autor de instrumento: **Caro Guzmán, Jonathan Martín**

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 apropiado													X
2.Objetividad	Se expresa la realidad como es, indica calidad de objetivo y la adecuación al objeto investigado.													X
3.Actualidad	Esta acorde a los aportes recientes al derecho													X
4.Organización	Existe una organización lógica													X
5.Suficiencia	Cumple con los aspectos metodológicos													X
6.Intencionalidad	Esta adecuado para valorar las categorías													X
7.Consistencia	Se respalda en fundamentos técnicos y científicos													X
8.Coherencia	Existe coherencia entre los problemas, objetivos, supuestos, basados en los aspectos teóricos y científicos.													X

9. Metodología	El instrumento responde al objetivo, diseño, tipo de la investigación.													X
10.Pertinencia	El instrumento tiene sentido frente a un problema crucial, está situado en una población, es interdisciplinaria, tiene relevancia global y asume responsablemente las consecuencias de sus hallazgos													X
														X

OPINIÓN DE APLICABILIDAD

- El instrumento cumple con los requisitos de para su aplicación — CUMPLE
- El instrumento cumple en parte con los requisitos para su aplicación — /
- El instrumento no cumple con los requisitos para su aplicación — /

PROMEDIO DE VALORACIÓN — 100%

Lima 14 de enero de 2026

ENRIQUE JORDAN LAOS JARAMILLO

DNI N°09911151-CelularN°997201314.

ANEXO G

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN II

VALIDACIÓN DEL INSTRUMENTO

I. DATOS GENERALES

1.1 Apellidos y Nombres: **GAMARRA RAMON JOSE CARLOS**

1.2 Cargo e institución donde labora: **Fiscal Provincial penal Lima Norte.**

1.3 Nombre del instrumento motivo de evaluación: Guía de entrevista

1.4 Autor del Instrumento: **Caro Guzmán, Jonathan Martín**

II. ASPECTOS DE VALIDACIÓN

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

III. OPINIÓN DE APLICABILIDAD

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

PROMEDIO DE VALORACIÓN: 95%

Lima, 07 de enero de 2026.

FIRMA DEL EXPERTO INFORMANTE
DNI N 09919088 Telf.: 973347510

ANEXO H

VALIDACIÓN DEL INSTRUMENTO DE INVESTIGACIÓN III

VALIDACIÓN DEL INSTRUMENTO

IV. DATOS GENERALES

1.4 Apellidos y Nombres: **PIEROLA VARGAS, OSCAR.**
1.5 Cargo e institución donde labora: **Abogado Especialista en Derecho Penal**
1.6 Nombre del instrumento motivo de evaluación: Guía de entrevista

1.4 Autor del Instrumento: **Caro Guzmán, Jonathan Martín**

V. ASPECTOS DE VALIDACIÓN

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

VI. OPINIÓN DE APLICABILIDAD

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

PROMEDIO DE VALOR 95%

Lima, 05 de enero de 2026.

DNI N° 33738966.
CelularN°98562535