UNIVERSIDAD DE HUANUCO

FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS

PROGRAMA ACADÉMICO DE DERECHO Y CIENCIAS POLÍTICAS

TESIS

“La incidencia del delito de fraude informático y la protección efectiva del ciudadano, distrito judicial de Huánuco, 2022 - 2023”

PARA OPTAR EL TÍTULO PROFESIONAL DE ABOGADA

AUTORA: Herrera Figueroa, Grecia Isabel

ASESOR: Guevara Vargas de Beraún, Erika Nilse

HUÁNUCO – PERÚ
2025

TIPO DEL TRABAJO DE INVESTIGACIÓN:

- Tesis (X)
- Trabajo de Suficiencia Profesional( )
- Trabajo de Investigación ( )
- Trabajo Académico ( )

LÍNEAS DE INVESTIGACIÓN: Derecho Administrativo

AÑO DE LA LÍNEA DE INVESTIGACIÓN (2020)

CAMPO DE CONOCIMIENTO OCDE:

Área: Ciencias Sociales
Sub área: Derecho
Disciplina: Derecho

DATOS DEL PROGRAMA:

Nombre del Grado/Título a recibir: Título Profesional de Abogada
Código del Programa: P33
Tipo de Financiamiento:

- Propio (X)
- UDH ( )
- Fondos Concursables ( )

DATOS DEL AUTOR:

Documento Nacional de Identidad (DNI): 47350447

DATOS DEL ASESOR:

Documento Nacional de Identidad (DNI): 22513448
Grado/Título: Maestra en Derecho y Ciencias Políticas, con mención en Derecho Procesal
Código ORCID: 0009-0006-9639-2468

DATOS DE LOS JURADOS:

N°	APELLIDOS Y NOMBRES	GRADO	DNI	Código ORCID
1	Ponce E Ingunza, Félix	Doctor en ciencias de la educación	22402569	0000-0003-0712-1414
2	Peralta Baca, Hugo Baldomero	Abogado	22461001	0000-0001-5570-7124
3	Minaya León, Jessica Juliana	Maestra en ciencias de la salud, salud pública y docencia universitaria	44256485	0009-0009-7932-4895

ACTA DE SUSTENTACIÓN DE TESIS

En la ciudad de Huánuco, siendo las 17.00 horas del día Diecinueve del mes de Diciembre del año dos mil veinticinco en cumplimiento de lo señalado en el Reglamento de Grados y Títulos de la Universidad de Huánuco, se reunieron la Sustentante y el Jurado calificador integrado por los docentes:

- **DR. FELIX PONCE E INGUNZA** : **PRESIDENTE**
- **ABOG. HUGO BALDOMERO PERALTA BACA** : **SECRETARIO**
- **MG. JESSICA JULIANA MINAYA LEON** : **VOCAL**
- **MG. YESSICA MARIA DE LOS ANGELES MACCHA ZAMBRANO** : **JURADO ACCESITARIO**
- **MG. ERIKA NILSE GUEVARA VARGAS DE BERAUN : ASESOR**

Nombrados mediante la Resolución N° 1398-2025-DFD-UDH de fecha 19 de Diciembre del 2025, para evaluar la Tesis titulada: **"INCIDENCIA DEL DELITO DE FRAUDE INFORMÁTICO Y LA PROTECCIÓN EFECTIVA DE CIUDADANO DISTRITO JUDICIAL DE HUÁNUCO 2022 - 2023"** presentado por la Bachiller en Derecho y Ciencias Políticas **GRECIA ISABEL HERRERA FIGUEROA** para optar el Título profesional de Abogada.

Dicho acto de sustentación se desarrolló en dos etapas: Exposición y Absolución de preguntas; procediéndose luego a la evaluación por parte de los miembros del jurado

Habiendo absuelto las objeciones que le fueron formuladas por los miembros del jurado y de conformidad con las respectivas disposiciones reglamentarias, procedieron a deliberar y calificar, declarándolo (a) aprobada Por unanimidad con el calificativo cuantitativo de quince y cualitativo de bueno

Siendo las 18.20 horas del día Diecinueve de Diciembre del año dos mil veinticinco los miembros del jurado calificador firman la presente Acta en señal de conformidad.

Dr. Félix Ponce e Ingunza
DNI: 22402569
CODIGO ORCID: 0000-0003-0712-1414
PRESIDENTE

Abog. Hugo Baldomero Peralta Baca
DNI: 22461001
CODIGO ORCID: 0000-0001-5570-7124
SECRETARIO

Mg. Jessica Juliana Minaya León
DNI: 44256485
CODIGO ORCID:0009-0009-7932-4895
VOCAL

VICERRECTORADO DE INVESTIGACIÓN

UNIVERSIDAD DE HUÁNUCO

CONSTANCIA DE ORIGINALIDAD

El comité de integridad científica, realizó la revisión del trabajo de investigación del estudiante: GRECIA ISABEL HERRERA FIGUEROA, de la investigación titulada "INCIDENCIA DEL DELITO DE FRAUDE INFORMÁTICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO DISTRITO JUDICIAL DE HUANUCO 2022 - 2023", con asesor(a) ERIKA NILSE GUEVARA VARGAS DE BERAUN, designado(a) mediante documento: RESOLUCIÓN N° 273-2025-DFD-UDH del P. A. de DERECHO Y CIENCIAS POLÍTICAS.

Puede constar que la misma tiene un índice de similitud del 24 % verificable en el reporte final del análisis de originalidad mediante el Software Turnitin.

Por lo que concluyo que cada una de las coincidencias detectadas no constituyen plagio y cumple con todas las normas de la Universidad de Huánuco.

Se expide la presente, a solicitud del interesado para los fines que estime conveniente.

Huánuco, 31 de octubre de 2025

UNIVERSIDAD DE HUÁNUCO
RESPONSABLE DE TURNITIN
HUÁNUCO - PERÚ

MANUEL E. ALIAGA VIDURIZAGA
D.N.I.: 71345687
cod. ORCID: 0009-0004-1375-5004

236. HERRERA FIGUEROA, GRECIA ISABEL.DOCX

INFORME DE ORIGINALIDAD

24%	23%	7%	13%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad de Huanuco Trabajo del estudiante	7%
2	repositorio.udh.edu.pe Fuente de Internet	3%
3	hdl.handle.net Fuente de Internet	2%
4	distancia.udh.edu.pe Fuente de Internet	2%
5	repositorio.unheval.edu.pe Fuente de Internet	2%
6	repositorio.usmp.edu.pe Fuente de Internet	1%
7	repositorio.uss.edu.pe Fuente de Internet	<1%
8	repositorio.usanpedro.edu.pe Fuente de Internet	<1%
9	Submitted to Universidad Tecnologica del Peru Trabajo del estudiante	<1%

UNIVERSIDAD DE HUÁNUCO
RESPONSABLE DE INTEGRIDAD CIENTÍFICA
HUÁNUCO - PERÚ

RICHARD J. SOLIS TOLEDO
D.N.I.: 47074047
cod. ORCID: 0000-0002-7629-6421

UNIVERSIDAD DE HUÁNUCO
RESPONSABLE DE TURNITIN
HUÁNUCO - PERÚ

MANUEL E. ALIAGA VIDURIZAGA
D.N.I.: 71345687
cod. ORCID: 0009-0004-1375-5004

DEDICATORIA

A Dios, por ser mi creador y porque me ha permitido terminar esta tesis; además por las bendiciones que a diario recibo de Él.

A mis padres y familiares, por todo su apoyo incondicional.

AGRADECIMIENTO

Mi profundo agradecimiento a mis padres porque en todo momento me han apoyado y creído en mí.

A mis familiares y amigos, por su apoyo incondicional y por no dejarme vencer frente a las adversidades.

A mis docentes de la Universidad de Huánuco, porque han forjado en mí el deseo de luchar siempre por la justicia y los derechos.

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

El objetivo general de la investigación fue describir el modo en que incidencia del delito de fraude informático se relaciona con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023; la tesis es jurídica de tipo aplicado, hermenéutico, bibliográfico y de campo, con un nivel o alcance descriptivo – explicativo; además el diseño fue correlacional y no experimental; la muestra de estudio fue no probabilística a intención de la tesista y correspondió a 10 casos fiscales correspondiente a los años de la investigación y que se encuentran concluidos y con requerimiento acusatorio, además de 10 fiscales de la Tercera Fiscalía Provincial Penal de Huánuco, especializada en delitos informáticos, con más de 3 años en el cargo, a los que se aplicó los instrumentos de recolección de datos; los resultados fueron sometidos al programa estadísticos SPSS 26, para hallar el coeficiente de correlación de Pearson, logrando comprobar las hipótesis formuladas, pues se ha encontrado una correlación positiva alta entre las variables de estudio, logrando establecer que en el caso de la hipótesis general existe un coeficiente de correlación de Pearson de 0,975, por ende, se logró demostrar que la que esta incidencia delictiva del delito de fraude informático tiene una relación negativa con la protección efectiva del ciudadano, ello a partir de las deficiencias de la actuación de los efectivos policiales, las actuaciones del fiscal de la investigación y las del juez penal mediante sus resoluciones, no protegen eficazmente al ciudadano.

Palabras clave. Delitos informáticos, fraude informático, investigación fiscal, patrimonio, resoluciones judiciales, víctima.

ABSTRACT

The general objective of the research was to describe how the incidence of the crime of computer fraud is related to the effective protection of citizens in the Judicial District of Huánuco, 2022 - 2023; the thesis is of an applied, hermeneutical, bibliographic and field legal nature, with a descriptive - explanatory level or scope; in addition, the design was correlational and not experimental; the study sample was non-probabilistic at the intention of the thesis student and corresponded to 10 fiscal cases corresponding to the years of the investigation and that are concluded and with an accusatory request, in addition to 10 prosecutors from the Third Provincial Criminal Prosecutor's Office of Huánuco, specialized in computer crimes, with more than 3 years in office, to which the data collection instruments were applied; The results were analyzed using SPSS 26 to determine the Pearson correlation coefficient. The hypothesis was tested, as a high positive correlation was found between the study variables. In the case of the general hypothesis, a Pearson correlation coefficient of 0.975 was established. Therefore, it was possible to demonstrate that the incidence of computer fraud is negatively related to the effective protection of citizens. This is due to the deficiencies in the actions of police officers, the actions of the investigating prosecutor, and the actions of the criminal judge through his resolutions, which do not effectively protect citizens.

Keywords: Computer crimes, computer fraud, tax investigation, assets, court rulings, victim.

INTRODUCCIÓN

El mundo dentro del contexto de los último 30 años, se ha visto inmerso en lo que se denomina la revolución informática ello desde la aparición del internet y la web, que obviamente es un medio útil para optimizar el sistema información, comunicación y almacenamiento de datos, lo que ha permitido, también el desarrollo de la globalización, tanto la informática y la tecnología ha permitido que tanto el hardware y software sean cada vez más sofisticados, pero al alcance de toda la población, tanto en las transacciones económicas, relaciones, transmisión de la información, lo que se ha incrementado en la época de pandemia y postpandemia, pues las actividades bancaria, comerciales, judiciales entre otras se han incrementado en el modo virtual.

Pero todas estas bondades, también han generado un lado negativo que se refleja en un problema evidente, que es la llamada ciber delincuencia o criminalidad informática, pues sujetos inescrupulosos se sirven de la informática, la tecnología y las redes de comunicación social para cometer una serie de conductas delictivas que afectan no solo a individuos como tales, sino a colectivos, sociedad e incluso al Estado.

Situación que es preocupante porque los delitos informáticos o ciber delitos, tienen una naturaleza muy especial, ya que es difícil poder determinar el lugar y la fecha de su comisión, además de poder establecer al sujeto activo del delito, ya que se comenten a través de plataformas digitales, programas informáticos desde distintos lugares del mundo, para cometer delitos cuyos efectos se producen en tiempo real y en diferentes partes del orbe, generando muchas veces la imposibilidad esclarecer la situación fáctica.

Frente a ello se tienen importantes convenios internacionales como el Tratado de Budapest, para enfrentar este delito desde un trabajo conjunto y articulado de los países, además dentro del derecho penal interno se tiene el Art. 8 de la Ley N. 30096 sobre delitos informáticos, respecto al delito de fraude informático, consiste en la conducta dolosa por medio de la cual el sujeto activo procura para sí o para otro un provecho ilícito, en perjuicio de

tercero mediante cualquiera de las siguientes conductas diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático; delito que protege el bien jurídico patrimonio; siendo que es una modalidad muy recurrente, pero a la vez difícil de investigar, razón por la cual a la tesista le surgió la idea de realizar una investigación en este tema, y se plateó como problema general: ¿De qué modo la incidencia del delito de fraude informático se relaciona con la protección efectiva del ciudadano, en el Distrito Judicial de Huánuco, 2022 - 2023?

La investigación se justica porque es un problema que necesita solución, además porque existen investigaciones extranjeras, nacionales y regionales que han tratado el tema, además de doctrina relevante sobre este tema; además luego de la investigación y comprobación de las hipótesis se plantea los prepuestos para la solución del problema, en beneficio del sistema de impartición de justicia penal dentro de la investigación de los delitos informáticos o ciber delitos, de otro lado para el desarrollo de la misma, la tesista ha elaborado sus propios instrumentos para la recolección de datos y los resultados fueron sometidos al programa estadístico SPSS 26, hallando en coeficiente de correlación de Pearson lo que ha permitido la comprobación de las hipótesis de estudio; por ende, los resultados son serios y tienen entidad científica; se debe indicar también, que en desarrollo de la tesis se ha observado de modo riguroso el Reglamento de Grados y Títulos de la Universidad de Huánuco, además se han empleado las Normas APA y los derechos de autor.

Entre las limitaciones más resaltante fueron poder encuestar a la muestra en una misma oportunidad, ya se tuvo que esperar a su disponibilidad, además muchos participantes no quisieron ser fotografiados ni que conste sus datos ya que son anónimas, pero todo fue superado por la responsable de la investigación.

CAPÍTULO I
PROBLEMA DE INVESTIGACIÓN

1.1. DESCRIPCIÓN DEL PROBLEMA

Durante los últimos 30 años el mundo ha sufrido una gran revolución informática, a partir de la creación de la web, como medio para mejorar el sistema de la información y comunicación, a la par que se ha producido el fenómeno de la globalización que ha sido coadyuvante para ello.

La informática y la tecnología, a través de hardware y software cada más más sofisticado, aunado al internet, ha facilitado el acceso a la información, el sistema de comunicación, almacenamiento de datos, sin que decir de las transacciones económicas, relaciones sociales se han ido incrementando, incluso durante la etapa de la pandemia y postpandemia el mundo comercial, bancario, ejecutivo, judicial, entre otros se han servido en el sistema del tele trabajo, la video conferencia e incluso la educación se realice virtualmente.

Pero pese a todas las bondades de la revolución cibernética o informática, también se ha presenta un problema muy serio y evidente, que es la ciber delincuencia, que se entiende como un fenómeno nocivo, en el cual sujetos se sirven de la informática, la tecnología y las redes de comunicación social para cometer una serie de conductas delictivas que afectan no solo a individuos como tales, sino a colectivos, sociedad e incluso al Estado.

Los delitos informáticos o ciber delitos, tienen una naturaleza muy especial, pues es muy difícil poder determinar el lugar y la fecha de su comisión, además de poder establecer al sujeto activo del delito, pues los delincuentes se sirven precisamente de la virtualidad así como de las plataformas digitales desde distintos lugares del mundo, para cometer delitos cuyos efectos se producen en tiempo real y en diferentes partes del orbe, generando muchas veces la imposibilidad esclarecer la situación fáctica; por ejemplo desde un barco en alta mar es decir, en aguas internacionales se puede crear una página web, aplicativo o plataforma digital, que sea una falsa aplicación de un banco nacional, que logre o permita acceder a cuentas de

los ahorristas, desde la cual se puede extraer el dinero y ser depositado en cuentas en paraísos fiscales, por ejemplo en Panamá, lo que dificultará hallar a los responsables, e incluso estas extracciones de dinero se realizan en contados segundos, lo que dificulta aún más la situación.

En este orden, en nuestro país se tiene el Art. 8 de la Ley N. 30096 sobre delitos informáticos, respecto al delito de fraude informático, consiste en la conducta dolosa por medio de la cual el sujeto activo procura para sí o para otro un provecho ilícito, en perjuicio de tercero mediante cualquiera de las siguientes conductas diseño, introducción, alteración, borrado, supresión, clonación de datos informáticos o cualquier interferencia o manipulación en el funcionamiento de un sistema informático; delito que protege el bien jurídico patrimonio; es importante considerar que en la actualidad la mayor incidencia de delitos contra el patrimonio se realizan dentro de la tipología de fraudes informáticos en la modalidad de clonación de datos informáticos y / o transferencias de datos de clientes de bancos que tienen tarjetas de crédito, y si bien se cuenta con la norma sustantiva que tipifica el delito, establece las modalidades delictivas y dispone de una sanción punitiva; así como también se tiene el Código Procesal Penal, que establece el procedimiento para la investigación criminal y juzgamiento, es importante investigar si realmente frente a la incidencia delictiva el Estado está en la capacidad de proteger de modo efectivo al ciudadano que es potencial víctima de este delito.

1.2. FORMULACIÓN DEL PROBLEMA

1.2.1. PROBLEMA GENERAL

PG. ¿De qué modo la incidencia del delito de fraude informático se relaciona con la protección efectiva del ciudadano, en el Distrito Judicial de Huánuco, 2022 - 2023?

1.2.2. PROBLEMAS ESPECÍFICOS

PE1. ¿Cómo se relaciona la actuación de la policía nacional del Perú en los delitos de fraude informático con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco 2022 - 2023?

PE2. ¿De qué forma las actuaciones del fiscal en la investigación por el delito de fraude informático se relaciona con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023?

PE3. ¿De qué modo las resoluciones dictadas por los jueces en los delitos de fraude informático se relacionan con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023?

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

OG. Describir el modo en que incidencia del delito de fraude informático se relaciona con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023.

1.3.2. OBJETIVOS ESPECÍFICOS

OE1. Determinar la relación de la actuación de la policía nacional del Perú en los delitos de fraude informático y la protección efectiva de la víctima en el Distrito Judicial de Huánuco 2022 - 2023

OE2. Establecer la forma en que las actuaciones del fiscal en la investigación por el delito de fraude informático se relacionan con la protección efectiva de la víctima en el Distrito Judicial de Huánuco, 2022 – 2023

OE3. Explicar el modo que las resoluciones dictadas por los jueces en los delitos de fraude informático se relacionan con la protección efectiva de la víctima en el Distrito Judicial de Huánuco, 2022 – 2023

1.4. JUSTIFICACIÓN DE LA INVESTIGACIÓN

1.4.1. JUSTIFICACIÓN PRÁCTICA

La justificación práctica de una investigación se encuentra referida a su aplicabilidad, en este sentido consideramos que la presente tesis tiene utilidad para resolver el problema investigados o plantear los presupuestos para resolver el mismo, (Martínez, 2020, p. 250), en este sentido, del desarrollo de la investigación y los resultados a los que se han arribado se ha logrado contrastar las hipótesis formuladas en su oportunidad, las mismas que resultan útiles para resolver, en beneficio del sistema de impartición de justicia penal dentro de la investigación de los delitos informáticos o ciber delitos.

1.4.2. JUSTIFICACIÓN METODOLÓGICA

La presente investigación tiene justificación metodológica, porque la investigadora ha elaborado sus propios instrumentos para la recolección de datos, los mismos que fueron debidamente tabulados y analizados y sometidos al Programa Estadístico SPSS 26, para lograr la comprobación de las hipótesis, (Martínez, 2020, p. 254), además porque para su desarrollo la tesista ha observado de modo riguroso la metodología de la investigación científica y el Reglamento de Grados y Títulos de la UDH

1.4.3. JUSTIFICACIÓN TEÓRICA

La presente investigación tiene justificación teórica porque para su elaboración y desarrollo la tesista ha contado con respaldo o sustento teórico y científico de otras investigaciones nacionales y extranjeras relativas al tema que han sido consignados como antecedentes; además para elaboración del marco teórico, la investigadora ha considerado la doctrina más relevante sobre la violencia de género, (Martínez, 2020, p. 249)

1.4.4. JUSTIFICACIÓN JURÍDICA

La presente investigación tiene justificación social, porque v ha se analizado problema que se presenta en el entorno social, (Martínez, 2020, p. 256), en este caso la ciber delincuencia y su relación con la investigación de los delitos informáticos.

1.5. LIMITACIONES DE LA INVESTIGACIÓN

Las limitaciones en una investigación han estado referidas a los obstáculos con los cuales se ha encontrado la investigadora durante el proceso del desarrollo de la investigación científica, (Zevallos, 2020, p. 129), uno de ellos fue encuestar a la muestra en una sola oportunidad, ya que por sus actividades profesionales la tesista tuvo que esperar su disponibilidad, además, muchos de los participantes no quisieron se encuestados porque, al ser anónima el cuestionario, se les solicitó que firmen y pongan sus datos en el consentimiento informado, a lo que se negaron devolviendo las encuestas, tuvimos que buscar otros participantes, muchos de ellos tampoco quisieron ser fotografiados.

Otra limitación es el tema económico porque la tesista no cuenta con beca ni subvención de entidad estatal o privada, por lo que los gastos que la investigación representó fueron asumidos en forma personal, además esta situación me ha limitados a realizar la investigación sólo en Huánuco.

CAPITULO II
MARCO TEÓRICO

2.1. ANTECEDENTES DE LA INVESTIGACIÓN

2.1.1. A NIVEL INTERNACIONAL

Echevarría (2010). Los delitos informáticos y el derecho constitucional a la seguridad pública. Tesis para optar el grado de maestro en Derecho Penal por la Universidad Técnica de Ambato, Ecuador.

La autora concluye que, en la actualidad el mundo ha ido cambiando, se evidencia una revolución tecnológica e informática, por ende los delitos ya no sólo se cometen dentro del mundo objetivo, sino también virtual, lo que genera una serie de efectos y desafíos para la seguridad ciudadana y estatal, las bondades del internet, también presenta un área negativa que corresponde a aquellas personas que aprovechándose o sirviéndose de la informática y tecnología comenten una serie de delitos, nocivos no solo respecto a sus efectos, sino también para lograr determinar a los autores, lugar de comisión, ello genera un desconcierto en los legisladores de establecer normas jurídicas para identificarlos y detenerlos, así también para hallar la evidencias, si bien el Código Penal ha tipificado estas conductas, aún se presentan problemas muy serios para investigar y sancionar, (Echevarría, 2015)

Peña (2023). Delitos cibernéticos. Tesis de la Universidad Libre de Colombia para obtener el grado de Maestro en Derecho Penal.

Según el citado autor, quien analiza la ciberdelincuencia desde el aspecto del sistema bancario, concluye que, si bien existen normas nacionales y tratados internacionales para la lucha contra la ciberdelincuencia, es necesario que se regulen lo protocolos nacional de acuerdo a los estándares establecidos en la legislación internacionales,

en concordancia al Tratado de Budapest, reconociendo que en Colombia se tienen diferencias tecnológicas y presupuestales, además se requiere de un trabajo conjunto y coordinado con todos los estados miembros para estar al frente en la lucha contra esta forma de criminalidad, se requiere la profesionalización y especialización de las actividades en criminalística y de investigación, que vaya de la mano con la evolución tecnológica, se quiere que las entidades financieras y bancarias dispongan de sistemas de seguridad modernos, pues son varios los bienes que vulneran o afectan estos delitos, (Peña, 2023)

2.1.2. A NIVEL NACIONAL

Villanueva (2023). En la tesis presentada para optar el título de abogado en la Universidad Señor de Sipán, se analiza el impacto de la Ley N. 30096 sobre delitos informáticos en la población de Chiclayo durante el periodo de la pandemia por la COVID-19. El estudio concluye que dicha normativa tuvo una influencia relevante en la comunidad, evidenciándose que, a través de conductas tipificadas como delitos informáticos, se vulneraron derechos fundamentales relacionados con la indemnidad y libertad sexual, así como con la intimidad personal y el secreto de las comunicaciones (Villanueva, 2023).

Carbajal, (2022). En la tesis presentada para obtener el grado de maestra en Ciencias Penales en la Universidad San Martín de Porres, se aborda el papel de las fiscalías especializadas en delitos informáticos como herramientas fundamentales en la lucha contra el ciberdelito. La autora concluye que entre los ilícitos más frecuentes en este ámbito destacan los fraudes informáticos y la clonación de tarjetas bancarias. Sin embargo, pese a la tipificación de estas conductas mediante la Ley N. 30096 y sus posteriores modificaciones, persisten limitaciones en el proceso investigativo. La División de Investigación de Alta Tecnología (DIAT) no cuenta con suficientes peritos especializados en esta forma de criminalidad, y gran parte de las víctimas no presentan denuncias, ya que los casos suelen resolverse directamente en las entidades

bancarias a través de reclamaciones o devoluciones monetarias. Además, la autora advierte deficiencias en los sistemas de seguridad de dichas instituciones. Otra dificultad relevante radica en la identificación de los responsables, lo que se complica por el uso de técnicas de encriptación y herramientas informáticas que facilitan el anonimato de los ciberdelincuentes, dificultando así su juzgamiento y sanción penal (Carbajal, 2022).

2.1.3. A NIVEL REGIONAL

Rivera (2022). Los delitos informáticos y su incidencia en la gestión de las instituciones del Estado del Distrito de Huánuco, 2017. Tesis para optar el grado de doctora en Derecho por la Universidad Nacional Hermilio Valdizán de Huánuco.

La autora señala que su investigación constituye un aporte significativo para la comunidad científica, ya que aborda de manera pionera la interrelación entre el Derecho y las Ciencias de los Sistemas e Informática. A través de su estudio, se evidencia que en las instituciones públicas del distrito de Huánuco existen tipificaciones inadecuadas de ciertos delitos, pues en muchos casos cualquier actuación de un funcionario público es considerada delictiva sin la debida delimitación jurídica. Asimismo, identifica vacíos legales que requieren ser subsanados mediante la modificación de la normativa vigente. La autora también resalta la necesidad de incorporar nuevas figuras delictivas, como la suplantación de identidad digital, la cual aún no ha sido reconocida ni tipificada en la actual legislación sobre delitos informáticos (Rivera, 2022).

Romero, (2021). En la tesis presentada para obtener el título de abogado en la Universidad de Huánuco, titulada Los delitos informáticos cometidos a través de las redes sociales y su tratamiento en el Ministerio Público en la ciudad de Huánuco (2016), la autora concluye que los delitos informáticos más frecuentes en dicha ciudad corresponden a la

alteración, daño o destrucción de bases de datos, el tráfico ilegal de información, los atentados contra la integridad de datos y sistemas informáticos, así como las proposiciones a menores de edad con fines sexuales mediante medios tecnológicos, la interceptación de datos informáticos, el fraude digital y la suplantación de identidad. No obstante, se advierte que más de la mitad de los casos investigados fueron archivados, mientras que solo una minoría llegó a ser judicializada y concluida con sentencia (Romero, 2021)

2.2. BASES TEÓRICAS

2.2.1. EL CIBER DELITO O DELITOS INFORMÁTICOS

El auge de la tecnología y la interconexión digital ha dado paso a un fenómeno global preocupante: el ciberdelito o llamado también los delitos informáticos; que es una forma de criminalidad, que se desarrolla en el vasto territorio del ciberespacio, plantea desafíos significativos para la seguridad, la privacidad y la estabilidad económica.

El ciberdelito se manifiesta en una variedad de formas, todas ellas aprovechando la omnipresencia de la tecnología digital, desde la sustracción de los datos personales hasta la extorsión en línea, pasando por la manipulación de información y el sabotaje digital, estos delitos representan una amenaza constante para individuos, empresas, instituciones y el propio Estado, (López, 2024, p. 131).

Entre las formas más recurrentes de estas conductas encontramos:

- **Robo de identidad y datos personales:** Los ciberdelincuentes buscan acceder ilegalmente a información confidencial, como nombres, direcciones, números de tarjetas de crédito y contraseñas (Ribón, 2024, p. 203).
- **Fraude en línea:** Se realizan estafas a través de internet, como la venta de productos falsificados o inexistentes, o la suplantación de identidad para obtener beneficios ilícitos (Ribón, 2024, p. 210).

- **Acoso cibernético:** Se emplean medios digitales para hostigar, intimidar o difamar a personas, a menudo a través de redes sociales, mensajes de texto o correo electrónico (Espinoza, 2023, p. 187).
- **Piratería informática:** Los hackers obtienen acceso no autorizado a sistemas informáticos con el fin de robar información, causar daños o interrumpir servicios (Vega & Arevalo, 2022, p. 89).
- **Difusión de malware:** Se distribuyen programas maliciosos diseñados para dañar sistemas informáticos, robar información o tomar control de dispositivos.
- **Ransomware:** Se cifran archivos o sistemas informáticos y se exige un rescate a cambio de su liberación, (Navagarces, 2022, p. 126).

Todas estas conductas generan una serie de impactos en la sociedad, pues no solo afecta a las víctimas directas, sino que también tiene consecuencias a nivel social, económico y político, entre los que encontramos

Impactos Individuales y Empresariales

- **Pérdida de privacidad y confianza:** Las víctimas pueden experimentar una invasión a su privacidad y sufrir daños psicológicos debido a la violación de su información personal.
- **Pérdidas económicas:** Las empresas pueden enfrentar pérdidas financieras significativas debido a la interrupción de servicios, el robo de propiedad intelectual o la responsabilidad legal por violaciones de datos, (Camacho, 2108, p. 137).

Además de los impactos Sociales y Políticos, tales como:

- **Desafíos para la seguridad nacional:** Los ciberataques pueden representar una amenaza para la infraestructura crítica de un país, como sistemas de energía, transporte o comunicaciones.
- **Desconfianza en la sociedad:** El aumento de los ciberdelitos puede minar la confianza en las instituciones y los servicios en línea, socavando la integridad del ciberespacio.

Frente a esta forma de criminales y por su especial naturaleza, se requiere que el Estado mediante el Derecho Penal y Procesal Penal, realice una serie de estrategias para hacerle frente, mediante una combinación de medidas técnicas, legales y de concienciación, entre ella se tiene:

La Cooperación Internacional: que es fundamental una colaboración estrecha entre países y agencias de aplicación de la ley para investigar y combatir el ciberdelito a nivel global.

La estandarización de protocolos y la compartición de información son esenciales para una respuesta efectiva.

El fortalecimiento de la seguridad cibernética, en tal sentido tanto las empresas y los individuos deben implementar medidas de seguridad cibernética robustas, como firewalls, cifrado de datos y autenticación de dos factores y la formación y la concienciación sobre seguridad son cruciales para mitigar el riesgo de ataques.

En el mismo sentido es importante contar con un marco legal, se necesitan leyes y regulaciones actualizadas que aborden específicamente el ciberdelito, incluyendo la protección de datos personales y la responsabilidad por violaciones de seguridad y disponer la previsión de penas y sanciones deben ser proporcionales a la gravedad del delito y disuasorias para los infractores, (Herrera, 2024).

Es conclusión, podemos afirmar que el ciberdelito es una amenaza persistente y en evolución que requiere una respuesta coordinada a nivel internacional. Solo mediante la cooperación entre gobiernos, empresas y ciudadanos, junto con la implementación de medidas técnicas y legales sólidas, podremos mitigar eficazmente este riesgo y salvaguardar la integridad del ciberespacio para las generaciones futuras.

2.2.2. EL TRATADO DE BUDAPEST

El Tratado de Budapest, también conocido como la Convención sobre Ciberdelincuencia del Consejo de Europa, representa un hito significativo en la respuesta internacional coordinada contra las amenazas cibernéticas, fue suscrito por muchos países, entre ellos el Perú en 2001 y entre en vigor a partir del 2004, este tratado establece un marco legal integral para abordar la ciberdelincuencia, promover la cooperación entre países y fortalecer la seguridad cibernética a nivel global, (Valencia, 2022, p. 216).

Uno de los aspectos más destacados del Tratado de Budapest es su énfasis en la cooperación internacional, pues reconoce que la ciberdelincuencia no se detiene en las fronteras y requiere una respuesta coordinada entre los estados. Alentar la asistencia legal mutua, el intercambio de información y la extradición de delincuentes es fundamental para investigar y enjuiciar eficazmente los delitos cibernéticos en un contexto transfronterizo.

El tratado proporciona una definición clara de una amplia gama de delitos cibernéticos, desde el acceso no autorizado a sistemas informáticos hasta el fraude informático y la explotación infantil en línea. Al establecer estándares mínimos para las leyes nacionales, ayuda a cerrar lagunas legales y garantizar que los estados tengan los instrumentos legales necesarios para combatir eficazmente la ciberdelincuencia (Gutiérrez, 2021, p. 301).

Otro aspecto fundamental del tratado es su enfoque en la protección de datos personales y la privacidad en línea. Reconoce la importancia de salvaguardar la información confidencial en el contexto de investigaciones sobre ciberdelitos, equilibrando la necesidad de seguridad con el respeto a los derechos individuales.

El tratado dedica una atención especial a la protección de los niños en línea, prohibiendo la producción y distribución de pornografía infantil

y estableciendo medidas para proteger a los menores de otros riesgos en línea. Este enfoque refleja la creciente preocupación por el bienestar de los niños en el entorno digital y la necesidad de medidas específicas para protegerlos, (Espinoza, 2023, p. 163).

Además de abordar la ciberdelincuencia, el Tratado de Budapest insta a los estados a promover la seguridad cibernética en general. Reconoce que la prevención es fundamental para reducir la vulnerabilidad a los ciberataques y fomenta la adopción de medidas técnicas y organizativas para fortalecer la resiliencia cibernética.

A pesar de sus numerosos logros, el Tratado de Budapest enfrenta desafíos en su implementación y aplicación efectiva. Las diferencias en las legislaciones nacionales y las limitaciones de recursos pueden obstaculizar la plena realización de sus objetivos. Sin embargo, sigue siendo un instrumento invaluable en la lucha contra la ciberdelincuencia, proporcionando un marco sólido para la cooperación internacional y el fortalecimiento de la seguridad cibernética a nivel mundial (Rivera, 2022, p. 211).

2.2.3. OTRAS NORMAS INTERNACIONALES CONTRA LA CIBER DELINCUENCIA

Entre las normas internacionales relativas a la ciber delincuencia, tienen las siguientes:

Directiva de la Unión Europea sobre la Seguridad de las Redes y la Información (NIS): establece normas comunes para la seguridad cibernética en la Unión Europea, con un enfoque particular en los sectores críticos. Para las universidades, esta directiva destaca la importancia de proteger la infraestructura de tecnología de la información y comunicación (TIC) contra amenazas como el ransomware y los ataques de denegación de servicio (DDoS). Además, fomenta la colaboración entre instituciones académicas y otros actores

del sector público y privado para mejorar la resiliencia cibernética, (Carbajal, 2022, p. 105).

Convención de las Naciones Unidas contra la Delincuencia Organizada Transnacional (UNTOC): Aunque la UNTOC no se centra exclusivamente en la ciberdelincuencia, proporciona un marco general para la cooperación internacional en la lucha contra la delincuencia organizada. Para las universidades, esto implica reconocer la importancia de abordar las actividades delictivas en línea, como la venta de drogas ilegales o la explotación infantil, que pueden tener ramificaciones tanto en el mundo físico como en el ciberespacio, (Espinoza, 2023, p. 184).

Directiva de la Unión Europea sobre la Lucha contra el Fraude y la Falsificación de Medios de Pago que no en Efectivo (PSD2): Se centra en la protección de los consumidores en el ámbito de los pagos electrónicos y transacciones financieras en línea. Aunque su impacto directo en las universidades puede ser limitado, destaca la importancia de implementar medidas de seguridad robustas en los sistemas de pago y la gestión financiera institucional para proteger contra el fraude en línea.

2.2.4. LEY N 30096. SOBRE DELITOS INFORMÁTICOS

La Ley N. 30096, conocida como: "Ley que modifica el Código Penal y establece agravantes y sanciones para los delitos informáticos y de alta tecnología", representa un hito significativo en la lucha contra los delitos informáticos en Perú. Esta legislación, promulgada con el objetivo de modernizar el marco legal y adaptarlo a los desafíos del ciberespacio, establece disposiciones clave para prevenir, investigar y sancionar los delitos informáticos en el país.

Define una amplia gama de acciones delictivas que constituyen delitos informáticos en Perú, que incluye el acceso no autorizado a sistemas informáticos, la interceptación de comunicaciones

electrónicas, la falsificación de datos informáticos y la producción de software malicioso, entre otros. La tipificación clara de estos delitos proporciona un marco legal sólido para abordar las actividades criminales en el ciberespacio, (Gutiérrez, 2021, p. 138).

La legislación establece agravantes y sanciones específicas para los delitos informáticos, reconociendo la gravedad de estas actividades y su impacto en la sociedad y la economía. Se imponen penas más severas cuando los delitos informáticos se cometen contra infraestructuras críticas o se relacionan con la comisión de otros delitos, como el fraude financiero o la trata de personas. Las sanciones pueden incluir penas de prisión, multas y otras medidas correctivas, proporcionando un elemento disuasorio importante contra la comisión de estos delitos.

También aborda la protección de datos personales y la privacidad en línea, reconociendo la importancia de salvaguardar la información confidencial en el ciberespacio. Establece disposiciones para proteger la confidencialidad, integridad y disponibilidad de la información personal almacenada en sistemas informáticos, así como para regular su procesamiento y tratamiento adecuado. Esto contribuye a fortalecer la confianza de los ciudadanos en el uso de tecnologías digitales y en la protección de su privacidad en línea (López, 2024, p. 211).

Además, incluye disposiciones para la cooperación internacional en la prevención, investigación y enjuiciamiento de delitos informáticos. Reconociendo la naturaleza transfronteriza de estos delitos, se fomenta el intercambio de información, la asistencia legal mutua y la colaboración entre países para combatir eficazmente la ciberdelincuencia. Además, se promueve la prevención a través de campañas de concientización pública, capacitación en seguridad informática y promoción de buenas prácticas en el uso de la tecnología.

En este sentido se puede afirmar que la Ley N. 30096 representa un avance significativo en la protección contra los delitos informáticos en

Perú, proporcionando un marco legal sólido para prevenir, investigar y sancionar estas actividades delictivas en el ciberespacio. Sin embargo, su implementación efectiva requerirá el compromiso y la colaboración de todos los actores involucrados, así como medidas complementarias, como la educación en seguridad informática y la cooperación internacional, para abordar de manera integral este desafío en la era digital, (Camacho, 2108, p. 169).

Esta norma ha establecido o tipificado una serie de delitos que se incorporan al Código Penal: todos ellos tienen como denominador común el uso indebido de tecnologías de la información y la comunicación, representan una preocupación creciente, siendo que se van a precisar los principales delitos informáticos en el país y las disposiciones legales que los regulan.

Acceso no autorizado a sistemas informáticos: Uno de los delitos informáticos más comunes es el acceso no autorizado a sistemas informáticos. Esto incluye intrusiones ilegales en redes corporativas, robo de información confidencial y manipulación de datos, (Herrera, 2024, p. 252). La Ley peruana establece sanciones para aquellos que realizan estas acciones sin consentimiento, protegiendo así la integridad de los sistemas y la privacidad de la información.

Interceptación ilegal de comunicaciones electrónicas: Es otra forma de delito informático, que abarca desde la intervención en correos electrónicos hasta el acceso no autorizado a conversaciones en línea. La legislación peruana prohíbe estas prácticas y establece medidas para su prevención y sanción, salvaguardando así la confidencialidad de las comunicaciones.

Falsificación de datos informáticos: Implica la manipulación o alteración de información digital con el propósito de engañar o causar perjuicio. Esto puede incluir la creación de documentos falsificados o la modificación de registros electrónicos (Gutiérrez, 2021, p. 301). La Ley peruana establece penas para quienes cometen este tipo de delitos,

protegiendo la integridad de la información y la confianza en los registros electrónicos.

Fraude informático: Conducta que involucra el uso de tecnologías de la información para cometer estafas o engaños. Esto puede incluir la suplantación de identidad en línea, la realización de transacciones fraudulentas o la difusión de contenido falso. La legislación peruana establece medidas para prevenir y sancionar este tipo de actividad delictiva, protegiendo así a los usuarios de internet.

Pornografía infantil en línea: Referida a la producción, distribución o posesión de material pornográfico que involucre a menores de edad es un delito grave en el Perú. La Ley peruana establece duras penas para quienes cometen este tipo de delitos, protegiendo así a los niños y adolescentes de la explotación y el abuso en línea, (Navagarces, 2022, p. 258).

Todos estos delitos informáticos representan una amenaza para la seguridad digital en el Perú. Sin embargo, la legislación peruana cuenta con disposiciones específicas para prevenir, investigar y sancionar estos delitos, protegiendo así a los ciudadanos y promoviendo un entorno digital seguro y confiable. Es importante continuar fortaleciendo estos marcos legales y promoviendo la concienciación sobre la seguridad digital para enfrentar eficazmente este desafío en el país.

2.2.5. DELITO DE FRAUDE INFORMÁTICO

En la actualidad, nuestra sociedad vive de la informática, depende de ella, la que se encuentra inserta en todos los niveles de actividad económica y financiera, la revolución informática y / o cibernética tiene incidencia en la economía, es decir en las transacciones económicas, pues los ciudadanos en su mayoría se sirven de los sistemas digitales para realizar sus transacciones para adquirir bienes y servicios, así como realizar sus actividades bancarias, cada vez es menos las situaciones en que las personas tienen dinero en metálico, sino que

habilitan sus cuentas bancarias a sus correos electrónicos y teléfono celulares, es más ya en menos ocasiones acuden a los bancos, pues desde sus dispositivos realizan todas sus transacciones, esta facilidad y bondades que proporciona la era digital, también ha ocasionado que aparezca o se consolide la delincuencia informática, siendo que los delincuentes cibernéticos o informáticos, buscan formas para apropiarse de dinero desde los sistemas digitales, (Villanueva, 2023, p. 111)

Se comete el delito de fraude informático se presenta cuando el autor del delito se vale de un sistema informático o de una terminal de un sistema de tratamiento de la información para cometer el ilícito penal, es un delito contra el patrimonio, por ende, se buscan cada vez formas más complejas de apropiarse de dinero ajeno, en tal sentido se tiene que gestionar sistemas de seguridad que protejan al ciudadano.

En nuestro país mediante la Ley N 30096 del 22 de octubre del 2013, se incorpora al sistema penal los delitos informáticos, derogando los Artículos 207 A al 207 D del Código Penal, que establece una serie de delitos informáticos, y en lo que respecta al fraude informático, como delito contra el patrimonio se encuentra tipificado en el Artículo 8 de la citada ley, como una conducta dolosa, mediante la cual el autor de modo deliberado e ilegítimo, es decir a sabiendas y sin tener derecho, genera para sí o para tercero un beneficio de índole económico, es decir, con ánimo de lucro, y como resultado se tiene el perjuicio del titular del bien jurídico, (Vega, 2022, p. 106)

El citado artículo precisa que esta conducta delictiva puede realizarse mediante las siguientes modalidades, que corresponden a los verbos rectores es decir, diseñar, introducir, borrar, alterar, suprimir, clonar datos informáticos, o mediante cualquier interferencia o manipulación en el funcionamiento del sistema informático, obviamente apropiarse del dinero del sujeto pasivo, siendo se agrava esta conducta si el sujeto pasivo es el Estado cuyo dinero es empleado para fines asistenciales o programas de apoyo social.

Este es un delito común, pues puede ser cometido por cualquier persona, obviamente que tenga los conocimientos y capacidades en sistemas digitales o de la información; es un delito doloso porque el sujeto activo tiene que actuar con conocimiento y voluntad de cometer el delito, además de ser un delito de resultados ya que debe causarse el perjuicio económico, es decir, el daño o menoscabo en el patrimonio del sujeto pasivo.

Actualmente, el delito de fraude informático es una de las conductas delictivas más dañinas, sin importar si el autor es una persona natural o una empresa, por cuanto los bienes jurídicos afectados serán igualmente penalizados. De otro lado, estos delitos son de alta ocurrencia en el mundo, ya que no solo se realizan en el escenario de las aulas universitarias o de los especialistas informáticos, sino que se ha convertido en una conducta que se ejerce en la cotidianeidad de los ciudadanos que, por practicidad, usan en muchas ocasiones el internet, (Romero, 2019, p. 201)

El fraude informático atenta contra el sistema y los datos almacenados; en ese sentido, el sistema y la confianza que se deposita en él forman parte de los requisitos inherentes del bien jurídico protegido. Por tanto, la actual tipificación del fraude informático en nuestro país resulta insuficiente para salvaguardarlo. Muchas veces, el acceso, cuando actúa sobre los datos, busca además dar a conocer el sistema o *liberar la información* para perjudicar a su titular, lo que origina un impacto en el patrimonio económico. Por lo que queda en claro que el bien jurídico no solo son los datos, sino la confianza depositada en el sistema. De otro lado, el tipo penal regula el acceso indebido generador de la acción fraudulenta, no considerando otra conducta que importe la acción de acceso que no tiene motivo propio.

El Código Penal establece penas y sanciones por los delitos derivados del fraude informático, dicha penalidad también implica aspectos patrimoniales, ya que el defraudado tiene derecho a ser resarcido económicamente del perjuicio que le causaron con el acto delictivo, como defraudados se consideran a los poseedores de bienes

o valores, en el caso de aquellos procedimientos denominados clásicamente como excesos de la banca y tecnológicamente como transacciones erradas, en ningún caso serán consideradas como una forma encubierta de financiar al cliente; toda vez que estas transacciones deben revertirse tal y como suceden, no son acumuladas a la cuenta del cliente "hasta encontrar una solución", (Ribón, 2024, p. 137)

2.2.6. LA PROTECCIÓN AL CIUDADANO

Frente a la incidencia de los delito de fraude informático se plantea la necesidad de proteger el patrimonio de los ciudadanos no sólo frente a situaciones de robos, hurtos o estafas, sino también ante la comisión de delito de fraude informático, por ende, genera la búsqueda de políticas protectoras que el Estado debe buscar, así como también las entidades bancarias, financieras o crediticias de emplear controles y sistemas de seguridad para encriptar sus datos e información, así como la los clientes y / o consumidores de sus productos como cuentas bancarias, tarjeras de ahorro, débito, crédito, asegurar la compra y transferencias virtuales, y desde las plataformas digitales, .

La mejor forma de contrarrestar el delito de fraude informático es a través de la prevención y está vinculada estrechamente con la seguridad, definida como aquello que evita un riesgo o peligro, dentro del ámbito informático, la seguridad se refiere a un estado que permite acceder a la información utilizando o modificando el hardware o el software. Los mecanismos y medidas utilizados en el campo informático a fin de evitar el fraude computacional son múltiples; algunas de ellas se encuentran en la denominada seguridad informática, la misma que es el conjunto de técnicas, herramientas y procedimientos que permiten asegurar un sistema de cómputo; buscando conservar la confidencialidad, la integridad, la disponibilidad y, sin duda, otros atributos de las partes o de la totalidad del sistema de cómputo, (Camacho, 2018, p. 213)

En el contexto de la seguridad, se menciona que el crimen organizado busca diversas formas de obtener dinero; sin embargo, el fraude informático se presenta como una forma de ganar dinero sin necesidad de hacer prácticamente esfuerzo intelectual, muchas conductas delictivas que se agrupan en el cibercrimen tienden normalmente a tener un mismo fin: el fraude.

Este es un riesgo en un mundo más globalizado, no deja de ser una ventana abierta a que las redes también sean utilizadas para delinquir y más aún por una población o ciudadanía que no está debidamente capacitada sobre el manejo correcto de este tipo de servicios, en el ámbito de negocios, la información es uno de los recursos más valorados, la información que fluye a través de los computadores y las redes de telecomunicaciones asociada a las operaciones comerciales o industriales es un conjunto de datos que tiene una importancia crítica para las organizaciones, características estas que sin duda algunas las hacen atractivas para la actividad ilegal, la facilidad con la que se puede compilar, analizar, manipular, acomodar y transmitir cantidades enormes de datos con una velocidad nunca antes experimentada, sitúa al fraude informático como un delito que no solo se comete con más frecuencia, sino que adquiere el mismo carácter transfronterizo que la comunicación electrónica, (Carbajal, 2022, p. 153)

Ello crea un espacio idóneo para cometer delitos de otra índole, crear identidades falsas, desviar fondos, introducir virus y, en general, atacar la privacidad y seguridad informática de usuarios y organizaciones, ya que el bioterrorismo informático es capaz de destruir en segundos miles de computadoras con información vital, directa o indirecta para los sistemas de seguridad.

2.2.7. LA LEY N 30171 Y SUS ALCANCES FRENTE A LOS DELITOS INFORMÁTICOS

En el ámbito de la protección del ciudadano se tiene la Ley N. 30171, también conocida como la Ley de Ciberseguridad, es una medida legislativa promulgada en Perú en julio de 2014 para abordar los desafíos emergentes en el ámbito de la ciberseguridad. Sus puntos clave son:

Esta norma, que modifica la Ley N. 30096, establece definiciones claras de conceptos relevantes en ciberseguridad y especifica su alcance, abarcando tanto entidades públicas como privadas que manejan sistemas de información dentro del territorio peruano.

Dispone la creación del Consejo Nacional de Ciberseguridad, (CONACIBER), que es un organismo encargado de diseñar políticas y estrategias para promover la ciberseguridad en Perú, además, fomenta la coordinación entre las diversas entidades involucradas en esta materia, es importante porque reconoce la importancia de las infraestructuras críticas para el funcionamiento del país, la ley establece medidas específicas para salvaguardar estos sistemas contra posibles amenazas cibernéticas, promueve la cooperación y coordinación entre entidades del sector público y privado, así como con organizaciones internacionales, con el objetivo de prevenir, detectar y responder eficazmente a incidentes de ciberseguridad, (Echevarría, 2015, p. 115).

La normativa insta a implementar programas de prevención y capacitación en ciberseguridad tanto a nivel público como privado, con el propósito de fortalecer la preparación y la resiliencia frente a potenciales amenazas digitales.

En resumen, podemos afirmar que representa un esfuerzo integral para mejorar la seguridad cibernética en el país, estableciendo un marco legal que busca proteger los activos digitales críticos y promover la colaboración entre los diferentes actores involucrados en este campo.

2.2.8. PROBLEMAS EN LA INVESTIGACIÓN DE DELITOS INFORMÁTICOS

En el contexto actual de rápida evolución tecnológica, los delitos informáticos representan una preocupación cada vez más apremiante para la seguridad cibernética a nivel global, la investigación de estos delitos representas una serie de desafíos complejos que requieren un enfoque multidisciplinario y altamente especializado.

Anonimato y rastreo digital: Uno de los principales desafíos en la investigación de delitos informáticos es el anonimato en línea y la dificultad para rastrear la identidad y la ubicación geográfica de los perpetradores. Las técnicas de anonimización, como el uso de redes privadas virtuales (VPN) y sistemas de enrutamiento en la red (TOR), dificultan la identificación de los responsables de los delitos cibernéticos, (Peña, 2023, p. 264).

Frente a ello se requiere desarrollar y aplicar metodologías avanzadas de análisis forense digital para rastrear la actividad delictiva en línea y determinar la identidad de los perpetradores con mayor precisión. Establecer colaboraciones con expertos en inteligencia digital y agencias de aplicación de la ley para mejorar las capacidades de investigación en este ámbito.

Complejidad Tecnológica y Actualización Constante: Los avances tecnológicos rápidos y continuos introducen nuevos desafíos en la investigación de delitos informáticos, además de la sofisticación de las herramientas y técnicas utilizadas por los delincuentes digitales, como el malware avanzado y las técnicas de ingeniería social, requiere que los investigadores estén constantemente actualizados y capacitados en las últimas tecnologías y metodologías de análisis forense digital, (Vega & Arevalo, 2022, p. 173), para ello es necesario establecer programas de educación continua y formación especializada en seguridad cibernética y análisis forense digital para investigadores de posgrado. Fomentar la colaboración con la industria y el sector privado para acceder a recursos y conocimientos técnicos de vanguardia.

La Jurisdicción y cooperación internacional: La naturaleza transfronteriza de los delitos informáticos plantea desafíos significativos en términos de jurisdicción y cooperación internacional. La falta de armonización legal entre países y los procedimientos complicados de extradición pueden obstaculizar la investigación y enjuiciamiento de delitos informáticos que trascienden las fronteras nacionales, (Villanueva, 2023, p. 183).

Para ello es importante promover la cooperación internacional y el intercambio de información entre agencias de aplicación de la ley, organismos gubernamentales y organizaciones internacionales. Fomentar la adopción de estándares comunes en materia de legislación y procedimientos legales para abordar la ciberdelincuencia a nivel global.

La investigación de delitos informáticos plantea dilemas éticos y desafíos relacionados con la protección de datos personales y la privacidad de los individuos. El manejo adecuado de la información sensible y el respeto a los derechos fundamentales de los usuarios de internet son aspectos críticos que deben tenerse en cuenta en la investigación de estos delitos, (Peña, 2023, p. 342).

Siendo necesario integrar principios éticos y consideraciones de privacidad en la planificación y ejecución de investigaciones de delitos informáticos. Establecer protocolos claros para el manejo y la protección de datos sensibles, así como mecanismos de supervisión y rendición de cuentas para garantizar el cumplimiento de estándares éticos y legales.

En tal sentido se afirma que la investigación de delitos informáticos en requiere un enfoque interdisciplinario, especializado y ético para abordar eficazmente los desafíos y complejidades inherentes a este campo.

2.2.9. FUNCIÓN DE LA FISCALÍA EN LA INVESTIGACIÓN DE CIBER DELITOS

En el contexto actual de la era digital, la fiscalía juega un papel crucial en la investigación de delitos informáticos, una forma cada vez más sofisticada de criminalidad que plantea desafíos únicos en términos de recolección de pruebas, identificación de autores y coordinación internacional. En este estudio de posgrado, se profundizará en la labor de la fiscalía en la investigación de delitos informáticos, destacando las complejidades y estrategias necesarias para abordar este fenómeno en evolución.

La gestión de denuncias y coordinación interinstitucional; se espera que la fiscalía asuma un rol proactivo en la gestión de denuncias relacionadas con delitos informáticos, implementando protocolos especializados para la recepción, clasificación y derivación de casos, (López, 2024, p. 200). Además, se enfatiza la importancia de la coordinación interinstitucional con unidades especializadas de la policía, agencias de inteligencia y organismos internacionales para maximizar los recursos y experticias disponibles en la investigación.

La fiscalía se distingue por su capacidad para liderar investigaciones avanzadas en delitos informáticos, haciendo uso de herramientas y técnicas de análisis forense digital de vanguardia, (Gutiérrez, 2021, p. 257). Esto implica la recolección, preservación y análisis de evidencia digital de manera rigurosa y científica, con el objetivo de reconstruir los eventos, identificar patrones de comportamiento y establecer la responsabilidad penal de los implicados.

La investigación de delitos informáticos plantea desafíos legales y jurisdiccionales complejos, especialmente cuando los actos delictivos trascienden las fronteras nacionales, por ende, se requiere que la fiscalía esté capacitada para abordar estos desafíos, navegando hábilmente a través de marcos legales internacionales, tratados de cooperación judicial y acuerdos de asistencia legal mutua para garantizar la efectividad de la investigación y enjuiciamiento.

Un aspecto fundamental en la labor de la fiscalía en la investigación de delitos informáticos es la protección de derechos fundamentales y el respeto a la ética jurídica. En el nivel de posgrado, se espera que la fiscalía adopte un enfoque ético y basado en principios en todas sus acciones, asegurando la integridad de la investigación, el cumplimiento de las normas de privacidad y la salvaguarda de los derechos de las partes involucradas, (Espinoza, 2023, p. 318).

En resumen, la función de la fiscalía en la investigación de delitos informáticos en el ámbito de posgrado va más allá de la aplicación de la ley, abarcando una amplia gama de responsabilidades y desafíos complejos. Mediante un enfoque multidisciplinario, ético y avanzado, la fiscalía de posgrado está capacitada para liderar la lucha contra la ciberdelincuencia, proteger los derechos de las víctimas y contribuir a la construcción de un entorno digital seguro y confiable en la sociedad moderna.

2.2.10. LA CRIMINALÍSTICA Y LA CIBER DELINCUENCIA

En la era digital, la criminalística juega un papel fundamental en la investigación de delitos informáticos, donde la complejidad y la sofisticación de las técnicas utilizadas requieren un enfoque avanzado y multidisciplinario.

La criminalística tiene la capacidad de identificar y reconocer la evidencia digital relevante de manera precisa y exhaustiva. Esto implica el uso de herramientas especializadas para detectar dispositivos de almacenamiento, registros de actividad en línea, archivos electrónicos y otros elementos digitales que puedan proporcionar información sobre el delito investigado, (Herrera, 2024, p. 293).

La recolección y preservación adecuada de la evidencia digital es fundamental para asegurar su integridad y autenticidad durante todo el proceso de investigación. En el ámbito de posgrado, la criminalística

emplea técnicas avanzadas de recolección de evidencia, como la creación de imágenes forenses, la copia bit a bit de dispositivos de almacenamiento y el registro detallado de la cadena de custodia, garantizando así la validez de la evidencia en el tribunal.

El análisis forense digital en el ámbito de posgrado requiere un enfoque avanzado y altamente especializado. Esto implica el uso de herramientas y técnicas avanzadas de análisis de datos, como el análisis de metadatos, la recuperación de datos borrados, el examen de registros de actividad y el análisis de malware. La criminalística en este nivel también se centra en la interpretación de la evidencia digital y la reconstrucción de los eventos relacionados con el delito de manera precisa y detallada, (Navagarces, 2022, p. 272).

La presentación de la evidencia digital en el proceso judicial es una tarea crítica que requiere habilidades avanzadas de comunicación y presentación. En el ámbito de posgrado, se espera que la criminalística elabore informes periciales detallados, utilice gráficos y diagramas para visualizar la información de manera clara y concisa, y participe como testigos expertos en el tribunal, explicando de manera experta la evidencia digital presentada.

Además de su papel en la investigación de casos específicos, la criminalística en el ámbito de posgrado también contribuye al avance del conocimiento en el campo de la seguridad cibernética y la prevención de delitos informáticos, (Valencia, 2022, p. 195). Esto puede incluir la realización de investigaciones académicas, el desarrollo de nuevas técnicas forenses digitales y la colaboración con agencias gubernamentales y empresas privadas en la formulación de políticas y estrategias de seguridad cibernética.

En resumen, la criminalística en la investigación de delitos informáticos en el ámbito de posgrado representa un enfoque avanzado y multidisciplinario que requiere habilidades y conocimientos especializados. A través de la aplicación de técnicas forenses digitales

avanzadas, la presentación experta de evidencia en el tribunal y la contribución al avance del conocimiento en el campo de la seguridad cibernética, la criminalística desempeña un papel crucial en la lucha contra la ciberdelincuencia y la protección de la seguridad digital en la sociedad moderna.

2.2.11. LA DIAT Y LA CIBERDELINCUENCIA

La Contribución de la División de Investigación de Alta Tecnología en la Lucha contra la Ciberdelincuencia en Perú, en el panorama actual de crecientes amenazas cibernéticas, la División de Investigación de Alta Tecnología (DIAT) en Perú desempeña un papel central en la prevención, detección y persecución de delitos informáticos. Este trabajo de posgrado profundiza en la función de la DIAT en la lucha contra la ciberdelincuencia, examinando sus estrategias, desafíos y perspectivas en este ámbito crítico, (Herrera, 2024, p. 311).

Investigación Avanzada de Delitos Informáticos, lleva a cabo investigaciones especializadas sobre una amplia gama de delitos informáticos, desde fraudes en línea hasta intrusiones cibernéticas, utilizando técnicas avanzadas de análisis forense digital para recopilar y analizar evidencia.

La DIAT trabaja en estrecha colaboración con agencias gubernamentales, organizaciones internacionales y empresas privadas para intercambiar información, recursos y mejores prácticas en la lucha contra la ciberdelincuencia, reconociendo la naturaleza transfronteriza de muchos delitos informáticos, (Espinoza, 2023, p. 285).

La DIAT invierte en el desarrollo profesional de su personal, proporcionando capacitación especializada en análisis forense digital, técnicas de investigación y seguridad cibernética avanzada para garantizar una respuesta efectiva a las amenazas cibernéticas emergentes.

Además de sus funciones investigativas, la DIAT participa en programas de prevención y sensibilización, educando al público y a las empresas sobre los riesgos de seguridad cibernética y promoviendo buenas prácticas en seguridad digital.

La rápida evolución de la tecnología presenta desafíos continuos para la DIAT en términos de adaptación a nuevas amenazas, adquisición de herramientas forenses actualizadas y mantenimiento de la competencia técnica de su personal.

La asignación adecuada de recursos financieros y humanos es crucial para el éxito de las operaciones de la DIAT, lo que requiere una gestión eficaz de recursos y un compromiso continuo por parte del gobierno y otras partes interesadas.

En conclusión, la DIAT desempeña un papel vital en la lucha contra la ciberdelincuencia en Perú, adoptando estrategias multidisciplinarias, invirtiendo en desarrollo de capacidades y colaborando estrechamente con otras agencias y organizaciones. Para garantizar su eficacia continua, es fundamental abordar los desafíos identificados y proporcionar el apoyo necesario para fortalecer su capacidad de respuesta frente a las amenazas cibernéticas en constante evolución, (Peña, 2023, p. 240).

2.3. DEFINICIONES CONCEPTUALES

- **Aplicativos informáticos.** Son programas informáticos diseñados como herramientas para realizar una serie de funciones específicas, diseñadas para realizar una serie de tareas complejas y hacer más sencillo la experiencia informática de los usuarios.
- **Evidencia.** La evidencia dentro del ámbito policial o fiscal, es un elemento que permite se contrastado para establecer con certeza la ocurrencia de un hecho o situación fáctica de interés en una investigación.

- **Digital.** Dentro del ámbito tecnológico o informático, este término incluye a todas las herramientas o soportes electrónicos, sistemas automáticos y recursos tecnológicos que son empleados para procesar y almacenar la información.

- **Hacker.** Es la denominación que se otorga a una persona que tiene conocimientos en informática y programación y, que en mérito a ello manipula o navega por el internet vulnerando los sistemas de seguridad.

- **Internet.** Se denomina así a la red global de computadoras interconectadas que permite el intercambio libre de la información entre todos sus usuarios a través de páginas web.

- **Página web.** Es un sitio web, es decir interconectado en el internet, que permite el intercambio de información en tiempo real y que puede acontecer para muchos sectores.

- **Redes sociales.** Son una serie de plataformas digitales que permiten la conexión e interacción entre los usuarios a través del internet, para recibir y enviar todo tipo de información.

- **Virtual.** Este concepto permite describir el universo que está en línea (on line), y no en la realidad física.

2.4. SISTEMA DE HIPÓTESIS

2.4.1. HIPÓTESIS GENERAL

HG. La incidencia del delito de fraude informático se relaciona de modo negativo con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023

Ho. La incidencia del delito de fraude informático no se relaciona de modo negativo con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023

2.4.2. HIPÓTESIS ESPECÍFICAS

HE1. La relación de la actuación de la policía nacional del Perú en los delitos de fraude informático no se relaciona eficazmente con la protección efectiva de la víctima en el Distrito Judicial de Huánuco 2022 - 2023

Ho. La relación de la actuación de la policía nacional del Perú en los delitos de fraude informático se relaciona eficazmente con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco 2022 – 2023

HE2. Las actuaciones del fiscal en la investigación por el delito de fraude informático no protegen de forma efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023

Ho. Las actuaciones del fiscal en la investigación por el delito de fraude informático protegen de forma efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023

HE3. Las resoluciones dictadas por los jueces en los delitos de fraude informático no protegen de modo efectivo del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023

Ho. Las resoluciones dictadas por los jueces en los delitos de fraude informático protegen de modo efectivo del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023

2.5. VARIABLES

2.5.1. VARIABLE INDEPENDIENTE

Vx. La incidencia del delito de fraude informático

2.5.2. VARIABLE DEPENDIENTE

Vy. Protección efectiva del ciudadano

2.6. OPERACIONALIZACIÓN DE VARIABLES

Tabla 1
Operacionalización de variables

Variables	Dimensiones	Indicadores
VI. Variable Independiente La incidencia del delito de fraude informático	- Actuación de la Policía Nacional del Perú. - Actuaciones del fiscal de la investigación	- Detención en flagrancia delictiva - Intervenciones a sospechosos - Recojo de evidencias
V.D. Variable Dependiente Protección efectiva de la víctima	Resoluciones del juez penal	- Investigaciones fiscales - Requerimiento de prisión preventiva - Acusaciones fiscales - Dictó prisión preventiva - Arribo a terminaciones anticipadas - Se dictó el auto de enjuiciamiento

CAPÍTULO III
METODOLOGÍA DE LA INVESTIGACIÓN

3.1. TIPO DE INVESTIGACIÓN

La presente investigación posee un enfoque jurídico, dado que se orienta al análisis de la aplicación de las normas legales vinculadas con los delitos de fraude informático y la protección efectiva de los ciudadanos (Romero, Palacios y Ñaupas, 2020, p. 432). Asimismo, se caracteriza por ser una investigación aplicada, ya que su propósito es proponer soluciones concretas a un problema existente en la sociedad (Zevallos, 2020, p. 135). Del mismo modo, el estudio adopta un enfoque hermenéutico, bibliográfico y de campo, lo que permite una comprensión integral del fenómeno jurídico desde la interpretación normativa, la revisión teórica y la observación directa de la realidad (Castillo, 2020, p. 278).

3.1.1. ENFOQUE DE LA INVESTIGACIÓN

El enfoque metodológico utilizado en esta investigación es de carácter cuantitativo, dado que la autora se centró en medir los indicadores correspondientes a cada variable mediante el uso de la estadística inferencial, con el propósito de comprobar las hipótesis planteadas (Martínez, 2020, p. 287). Para ello, se aplicó el método deductivo, el cual se basa en un razonamiento que parte de conceptos generales para llegar a conclusiones específicas (Castillo, 2020, p. 373).

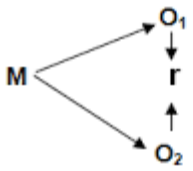
3.1.2. ALCANCE O NIVEL DE LA INVESTIGACIÓN

Es descriptivo – explicativo, ya que la tesista ha descrito el problema, para ello ha descompuesto el fenómeno en cada una de sus características y luego de obtener los resultados se ha procedido a la comprobación las hipótesis, de lo cual se ofrece una explicación del mismo, (Romero, Palacios, & Ñaupas , 2020, p. 444)

3.1.3. DISEÑO DE INVESTIGACIÓN

Es correlacional, pues el propósito fue de establecer la relación entre las variables de estudio, es decir, la variable independiente y la dependiente, (Hernández, 2014, p. 48), además, no experimental porque la tesista no ha manipulado las variables, ya que realizó la observación y análisis de las mismas, y como se presentan, (Cazau, 2006, p. 134)

Tabla 2
Esquema de la investigación correlacional



Donde:

M = Muestra

O_1 = Observación de la V.1.

O_2 = Observación de la V.2.

r = Correlación entre dichas variables.

3.2. POBLACIÓN Y MUESTRA

3.2.1. POBLACIÓN

La población estuvo conformada por lo siguiente:

Tabla 3
Población

Característica	Descripción	Cantidad
Sujetos	Fiscales de la Tercera Fiscalía Provincial Penal Corporativa de Huánuco especializada en delitos Informáticos	16
Casos	Casos investigados por delito de fraude informático de los años 2022 - 2023	56
	Total	72

3.2.2. MUESTRA

Entendemos por muestra a la parte del universo o población con la cual se desarrolló la investigación, por lo tanto, es una porción representativa de un grupo poblacional.

Para tal efecto la investigadora ha optado por el método no probabilístico para obtener la cantidad de muestra, contará con la cantidad de 10 fiscales y 10 casos investigados

3.2.3. CRITERIOS DE INCLUSIÓN Y EXCLUSIÓN

La muestra seleccionada en esta investigación fue de tipo no probabilística**,** determinada según el criterio intencional de la investigadora**.** Para su conformación, se establecieron los siguientes criterios de inclusión**:** en primer lugar, se consideró a los fiscales titulares que cuentan con más de tres años de experiencia en el ejercicio del cargo**;** y en segundo lugar, se incluyeron casos en etapa de conclusión de la investigación**,** específicamente aquellos que presentan requerimiento acusatorio**.**

Tabla 4
Muestra

Característica	Descripción	Criterios de inclusión	Criterios de exclusión	Cantidad
Sujetos	Fiscales de 3 F.P.P.C. Huánuco, especializada en delitos informáticos	Titulares en el cargo con más de 3 años en la función	No se tomó como muestra a fiscales provisionales, ni aquellos que tengan menos de 3 años en el cargo aun sean titulares por no tener mayor experiencia	10
Casos	Investigaciones por delito de fraude informático correspondiente al año 2022 - 223	Investigaciones en conclusión de investigación preparatoria con requerimiento de acusación	No se tuvo en cuenta como muestra los casos que estén aun en investigación	10
Total				20

3.3. TÉCNICAS E INSTRUMENTOS PARA LA RECOLECCIÓN DE DATOS

3.3.1. TÉCNICAS DE RECOLECCIÓN DE DATOS

Se han empleado las siguientes técnicas de recolección de datos

- **Fichaje.** Que, aplicó sobre los textos, artículos e investigaciones, con la finalidad de organizar el desarrollo y elaboración del marco teórico
- **Encuesta.** La misma que fue aplicada a la muestra de estudio conformada por los fiscales de la fiscalía especializada en delitos informáticos a fin de recabar su opinión.
- **Observación y análisis de casos.** Que, fue aplicada sobre los casos investigados de delito de fraude informático que va a conformar la muestra.

3.3.2. INSTRUMENTOS DE RECOLECCIÓN DE DATOS

Se han empleado los siguientes instrumentos:

- **Fichas.** Tanto bibliográficas, de transcripción y de resumen.
- **Cuestionario.** Que, contiene una serie de preguntas con un rango de respuestas o alternativas politómicas cerradas, para conocer la opinión de la muestra, de acuerdo a la siguiente escala de Likert.

Tabla 5
Tabla de Likert

Alternativas	Valor
Siempre	5
Casi siempre	4
Indiferente	3
Casi nunca	2
Nunca	1

Matriz de análisis. Para obtener los casos de los casos investigados.

3.3.3. VALIDACIÓN DE INSTRUMENTOS

Los instrumentos que se han aplicado a la muestra de estudio, han sido elaborados por la propia investigadora, han sido debidamente validados por 3 expertos, docentes universitarios del área de derecho e investigación científica, como se adjunta en el anexo correspondiente.

3.3.4. CONFIABILIDAD DE INSTRUMENTOS

Se realizó una prueba piloto aplicando la encuesta a 5 sujetos que no han integrado la investigación, se efectuó la prueba de confiabilidad por el sistema Alfa de Cronbach, obteniendo como resultado el siguiente:

Tabla 6
Prueba de Alfa de Cronbach

$$\alpha = \frac{K}{K-1}\left(\frac{\sum_{i=1}^{K}\sigma_{Y_i}^2}{\sigma_X^2}\right)$$

α (ALFA) =	**0.88705234**
K (NUMERO DE ITEMS) =	6
∑Vi (VARIANZA DE CADA ITEM)=	11.84
Vt (VARIANZA TOTAL) =	63.36

De acuerdo con los resultados obtenidos en la prueba de confiabilidad**,** el coeficiente Alfa de Cronbach alcanzó un valor de 0.887**,** lo que indica un nivel de consistencia interna alto y, por tanto, una adecuada fiabilidad para proceder con la aplicación de los instrumentos de investigación**.**

3.4. TÉCNICAS PARA EL PROCESAMIENTO Y ANÁLISIS DE LA INFORMACIÓN

Luego de recolección de datos, los resultados han sido debidamente ordenados y tabulados en una base de datos, tanto del cuestionario como de

la guía de análisis de casos, para luego ser sometidos al programa estadístico que permitió la obtención de los resultados, que serán presentados en tablas y figuras y la interpretación y análisis correspondiente.

Los resultados obtenidos fueron procesados utilizando técnicas de estadística inferencial, empleando para ello el software estadístico SPSS versión 26**.** Este análisis permitió calcular el coeficiente de correlación de Pearson**,** a través del cual se determinó la relación existente entre las variables de estudio y, en consecuencia, se procedió a la comprobación de las hipótesis planteadas**.**

Siendo que en el desarrollo de la presente tesis se trabajó con una muestra conformada por sujetos, (fiscales), se contó con el consentimiento informado de los mismos, además la tesista guarda absoluta reserva de la identidad de estos, cuyo formato se adjunta en los anexos.

Por otra parte, la tesista ha respetado los derechos de autor, efectuando las citas y referencias de acuerdo con las Normas APA última versión.

CAPITULO IV

RESULTADOS

4.1. DESCRIPCIÓN DE LA REALIDAD OBSERVADA

4.1.1. RESULTADOS DE LA DIMENSIÓN ACTUACIÓN DE LA POLICÍA NACIONAL DEL PERÚ

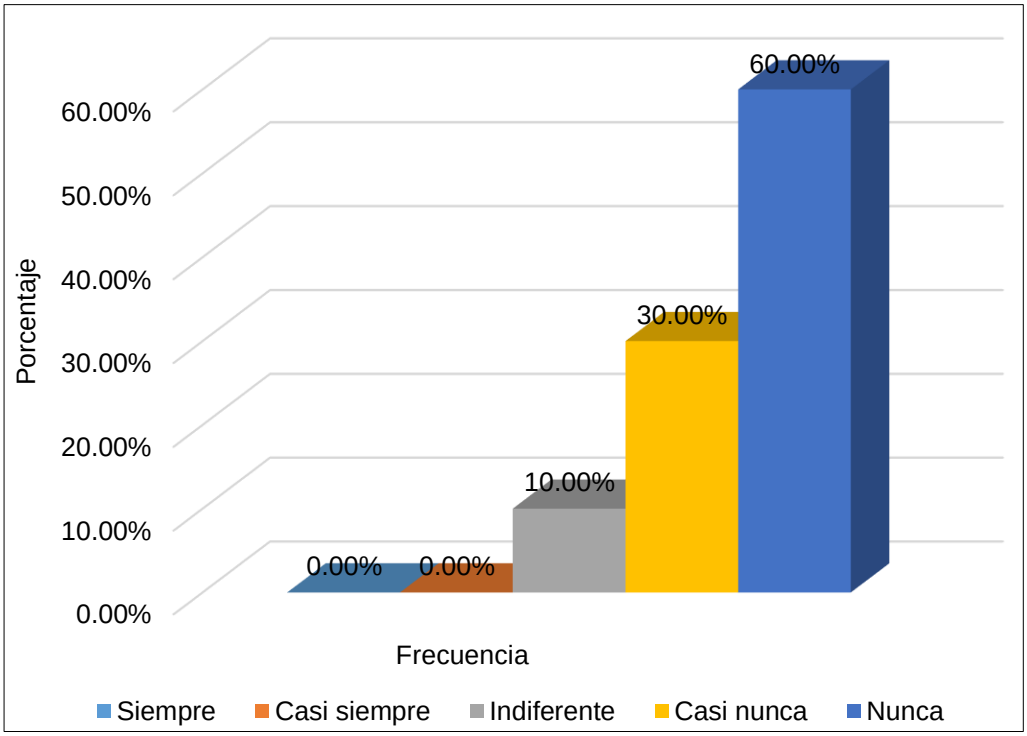
Tabla 7

Pregunta 1. ¿La Policía Nacional del Perú detuvo en flagrancia al autor y partícipes del delito?

Alternativa	f	%	Fi
Siempre	0	0.0%	0.0%
Casi siempre	0	0.0%	0.0%
Indiferente	1	10.0%	10.0%
Casi nunca	3	30.0%	30.0%
Nunca	6	60.0%	60.0%
Total	10	100.0%	100.0%

Figura 1

Pregunta 1. ¿La Policía Nacional del Perú detuvo en flagrancia al autor y partícipes del delito?



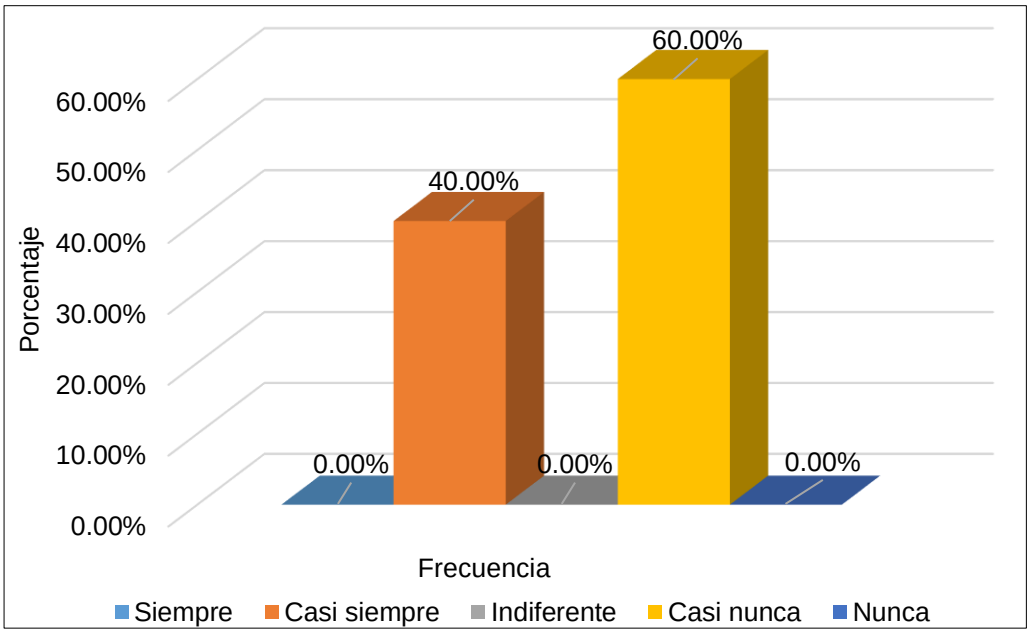
Interpretación y análisis de resultados

La primera pregunta fue para conocer su opinión si personal policial detuvo en flagrancia al imputado, al respecto el 60.00% dijo nunca, el 30.00% casi nunca y el 10.00% que es indiferente, de estos resultados se colige que, en los delitos de fraude informático, por la misma modalidad en que se comete desde un servidor o computadora, son muy pocas las situaciones en las que se detienen al autor o partícipe en situación de flagrancia delictiva.

Tabla 8
Pregunta 2. ¿La Policía Nacional del Perú intervino a sospechosos del delito?

Alternativa	f	%	Fi
Siempre	0	0.0%	0.0%
Casi siempre	2	20.0%	20.0%
Indiferente	0	0.0%	0.0%
Casi nunca	0	0.0%	0.0%
Nunca	8	80.0%	80.0%
Total	10	100.0%	100.0%

Figura 2
Pregunta 2. ¿La Policía Nacional del Perú intervino a sospechosos del delito?



Interpretación y análisis de resultados

La segunda pregunta fue para conocer si la Policía Nacional del Perú intervino a sospechosos del delito, al respecto el 60.00% dijo casi nunca y el 40.00% casi siempre, de ello se colige que en la mayoría de casos no se interviene a los sospechosos, ello por la forma como se comete el delito, lo que si ocurre en pocos casos.

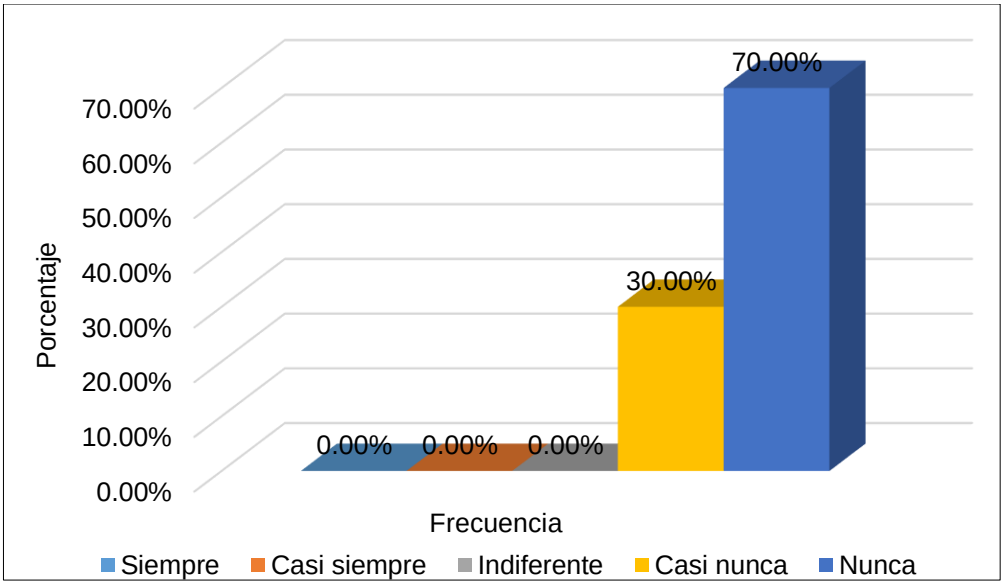
Tabla 9

Pregunta 3. ¿La Policía Nacional del Perú cuenta con la especialización en el recojo de evidencias del delito de fraude informático?

Alternativa	f	%	Fi
Siempre	0	0.0%	0.0%
Casi siempre	0	0.0%	0.0%
Indiferente	0	0.0%	0.0%
Casi nunca	3	30.0%	30.0%
Nunca	7	70.0%	70.0%
Total	10	100.0%	100.0%

Figura 3

Pregunta 3. ¿La Policía Nacional del Perú cuenta con la especialización en el recojo de evidencias del delito de fraude informático?



Interpretación y análisis de resultados

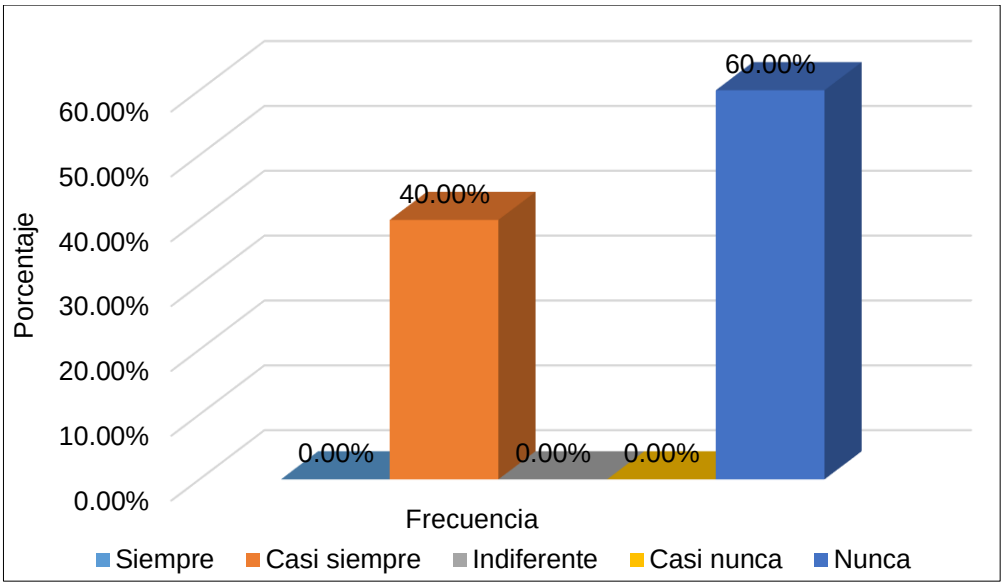
La tercera pregunta fue para conocer si la Policía Nacional del Perú cuenta con la especialización en el recojo de evidencias del delito de fraude informático, al respecto el 70.00% dijo que nunca y el 30.00% casi nunca, de ello se desprende que no se recogen las evidencias de modo correcto, porque los efectivos policiales encargados no cuentan con la especialización en criminalista informática, tampoco ayuda los pocos recursos logísticos de la institución policial.

4.1.2. RESULTADOS DE LA DIMENSIÓN: ACTUACIÓN DEL FISCAL DE LA INVESTIGACIÓN

Tabla 10
Pregunta 4. ¿La investigación fiscal fue la adecuada?

Alternativa	F	%	Fi
Siempre	0	0.0%	0.0%
Casi siempre	4	40.0%	40.0%
Indiferente	0	0.0%	0.0%
Casi nunca	0	0.0%	0.0%
Nunca	6	60.0%	60.0%
Total	10	100.0%	100.0%

Figura 4
Pregunta 4. ¿La investigación fiscal fue la adecuada?



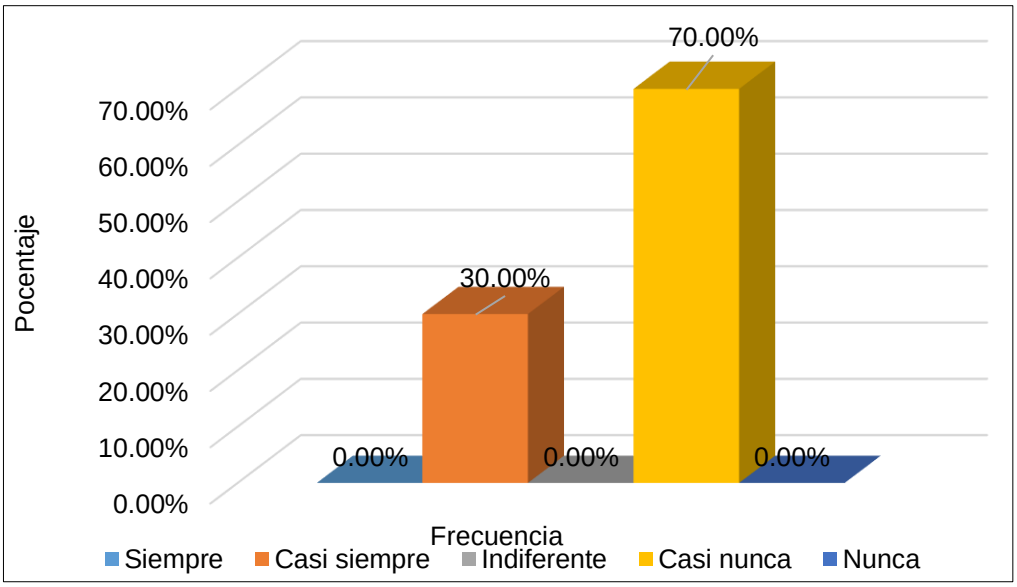
Interpretación y análisis de resultados

La cuarta pregunta fue para conocer la opinión si la investigación fiscal fue la adecuada, al respecto el 60.00% dijo nunca y el 40.00% casi siempre, de ello se colige que la mayoría considera que la investigación fiscal en casos de delitos de fraude informático no es adecuada, ello se colige también con la observación y análisis de casos donde se ha verificado tal situación.

Tabla 11
Pregunta 5. ¿El fiscal requirió la prisión preventiva del autor?

Alternativa	F	%	Fi
Siempre	0	0.0%	0.0%
Casi siempre	3	30.0%	30.0%
Indiferente	0	0.0%	0.0%
Casi nunca	7	70.0%	70.0%
Nunca	0	0.0%	0.0%
Total	10	100.0%	100.0%

Figura 5
Pregunta 5. ¿El fiscal requirió la prisión preventiva del autor?



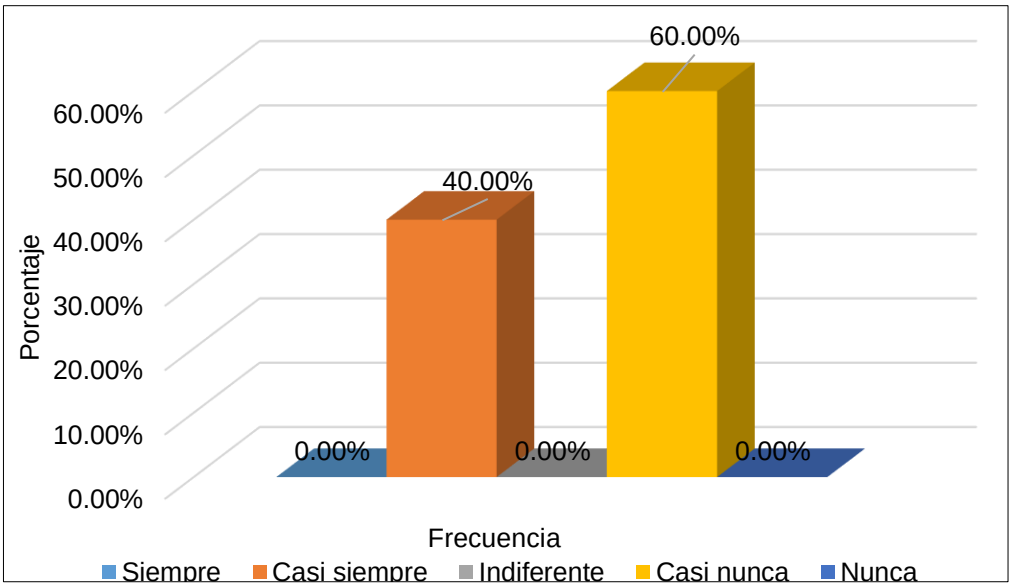
Interpretación y análisis de resultados

La quinta pregunta fue para conocer su opinión si el fiscal requirió la prisión preventiva del autor, al respecto el 70.00% dijo casi nunca y el 30.00% casi siempre, de ello se colige que con muy pocos en los cuales se solicita la prisión preventiva y ello ocurre porque el autor no fue intervenido en flagrancia, porque no se reunieron las evidencias o elementos de convicción e incluso por la deficiente investigación.

Tabla 12
Pregunta 6. ¿El fiscal requirió la acusación fiscal?

Alternativa	F	%	Fi
Siempre	0	0.0%	0.0%
Casi siempre	4	40.0%	40.0%
Indiferente	0	0.0%	0.0%
Casi nunca	6	60.0%	60.0%
Nunca	0	0.0%	0.0%
Total	10	100.0%	100.0%

Figura 6
Pregunta 6. ¿El fiscal requirió la acusación fiscal?



Interpretación y análisis de resultados

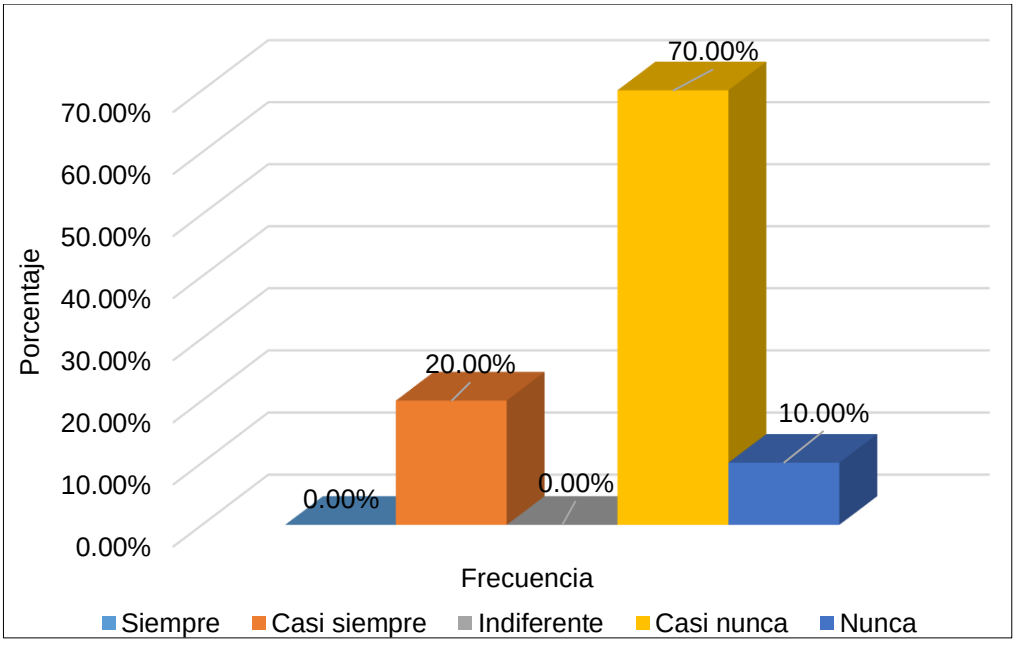
La sexta pregunta fue para conocer su opinión si el fiscal requirió la acusación fiscal, al respecto se tiene que el 60.00% dijo casi nunca y el 40.00% casi siempre, de los resultados se colige que con muy pocas veces en las cuales el fiscal requiere la acusación fiscal por delito de fraude informático, ello se debe porque no se interviene a los sospechosos, no se realiza un adecuado recojo de evidencias y la investigación fiscal es deficiente.

4.1.3. RESULTADOS DE LA DIMENSIÓN: RESOLUCIONES DEL JUEZ PENAL

Tabla 13
Pregunta 7. ¿El juez dictó prisión preventiva al autor y / o partícipes?

Alternativa	F	%	Fi
Siempre	0	0.0%	0.0%
Casi siempre	2	20.0%	20.0%
Indiferente	0	0.0%	0.0%
Casi nunca	7	70.0%	70.0%
Nunca	1	10.0%	10.0%
Total	10	100.0%	100.0%

Figura 7
Pregunta 7. ¿El juez dictó prisión preventiva al autor y / o partícipes?



Interpretación y análisis de resultados

La séptima pregunta fue para conocer si el juez dictó prisión preventiva al autor y / o partícipes, de los resultados se tiene que el 70.00% respondió casi nunca, el 10.00% dijo nunca y el 20.00% casi siempre, al respecto se tiene que son muy pocos los casos en los que se ha requerido prisión preventiva, siendo que estos resultados son coherentes con la observación y análisis de casos.

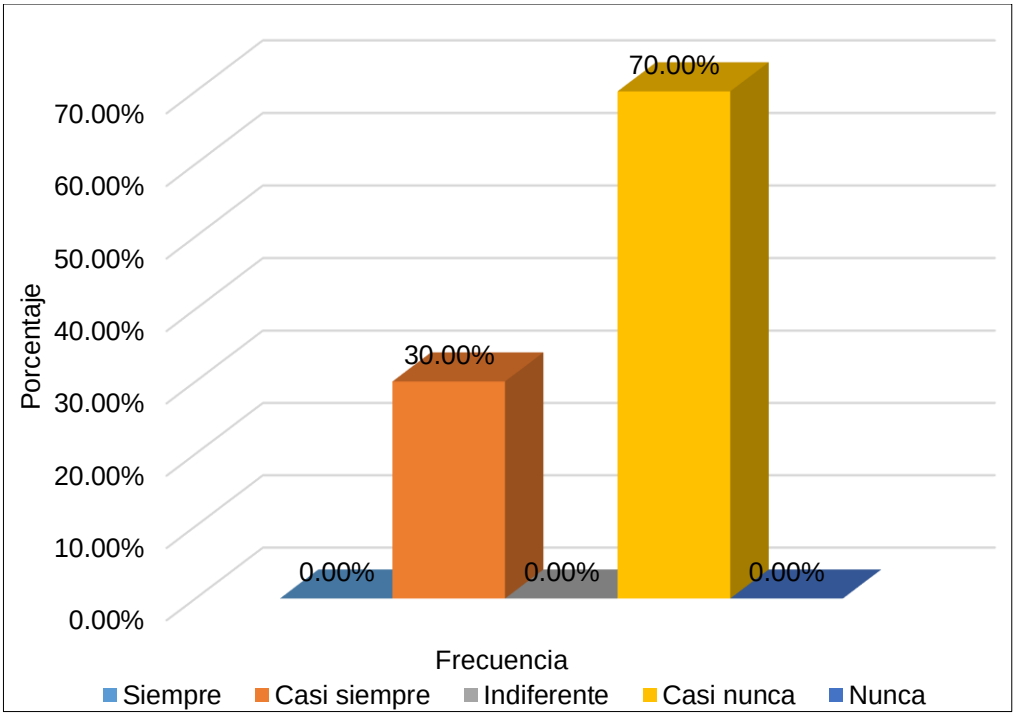
Tabla 14

Pregunta 8. ¿Se arribaron a terminaciones anticipadas con el resarcimiento de la víctima?

Alternativa	F	%	Fi
Siempre	0	0.0%	0.0%
Casi siempre	3	30.0%	30.0%
Indiferente	0	0.0%	0.0%
Casi nunca	7	70.0%	70.0%
Nunca	0	0.0%	0.0%
Total	10	100.0%	100.0%

Figura 8

Pregunta 8. ¿Se arribaron a terminaciones anticipadas con el resarcimiento de la víctima?



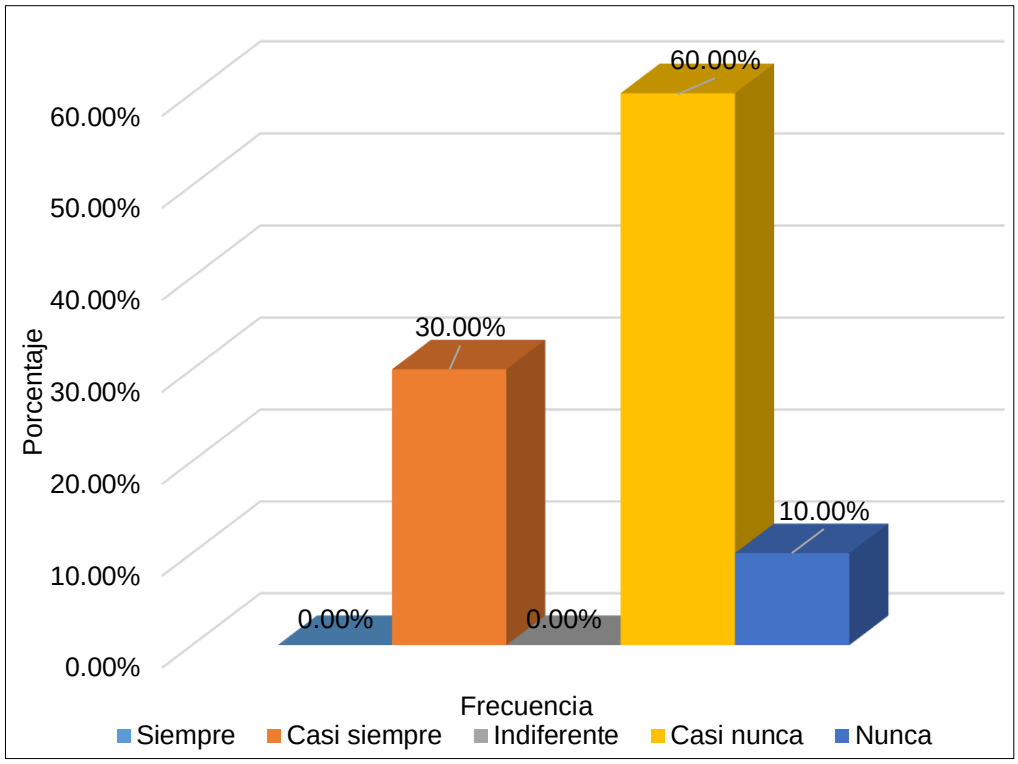
Interpretación y análisis de resultados

La octava pregunta fue para conocer su opinión si se arribaron a terminaciones anticipadas con el resarcimiento de la víctima, al respecto se tiene que el 70.00% dijo casi nunca y el 30.00% casi siempre, de ello se colige que con poco los casos en los cuales se llegó a la terminación anticipada con el resarcimiento a la víctima, estos resultados también se coligen con los obtenidos de la observación y análisis de casos.

Tabla 15
Pregunta 9. ¿El juez emitió el auto de enjuiciamiento?

Alternativa	F	%	Fi
Siempre	0	0.0%	0.0%
Casi siempre	3	30.0%	30.0%
Indiferente	0	0.0%	0.0%
Casi nunca	6	60.0%	60.0%
Nunca	1	10.0%	10.0%
Total	10	100.0%	100.0%

Figura 9
Pregunta 9. ¿El juez emitió el auto de enjuiciamiento?



Interpretación y análisis de resultados

La novena pregunta fue para conocer su opinión si el juez emitió el auto de enjuiciamiento, de ello se desprende que en el 60.00% dijo casi nunca, el 10.00% nunca y el 30.00% casi siempre, de ello se colige que en muy pocos casos se ha dictado en auto de enjuiciamiento lo que también está de acuerdo con los resultados de la observación y análisis de casos.

4.1.4. RESULTADOS DE LA OBSERVACIÓN Y ANÁLISIS DE CASOS

Tabla 16

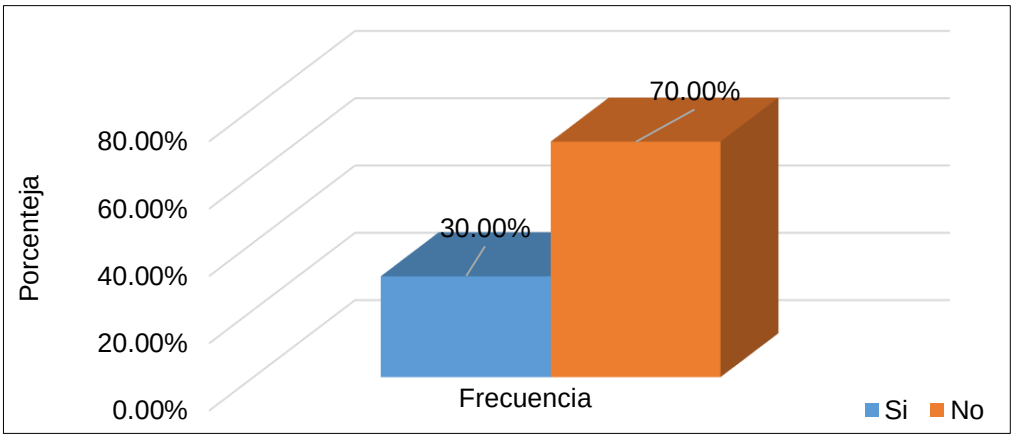
Observación y análisis de casos

N.	N. Carpeta Fiscal	Actuaciones de la Policía Nacional del Perú			Actuaciones del fiscal en la investigación			Resoluciones del Juez Penal		
		Detención en flagrancia	Intervención a sospechosos	Recojo de evidencias	Investigación fiscal suficiente	Requerimiento de prisión preventiva	Acusaciones fiscales	Auto de prisión preventiva	Terminación anticipada	Auto de enjuiciamiento
1	135-2022	No	Si	Si	No	No	Si	No	No	No
2	212-2022	Si	Si	Si	No	Si	No	Si	Si	No
3	346-2022	No	No	No	No	No	No	No	No	No
4	531-2022	Si	Si	No	No	No	No	No	No	No
5	628-2022	No	No	Si	Si	No	Si	No	Si	Si
6	667-2022	No	No	No	No	No	No	No	No	No
7	147-2023	Si	Si	Si	Si	No	Si	No	No	Si
8	276-2023	No	Si	No	No	Si	Si	Si	No	Si
9	305-2023	No	No	No	No	No	No	No	No	No
10	326-2023	No	No	No	No	No	No	No	No	No

Nota. Casos observados

1. Dimensión: Actuaciones de la Policía Nacional del Perú

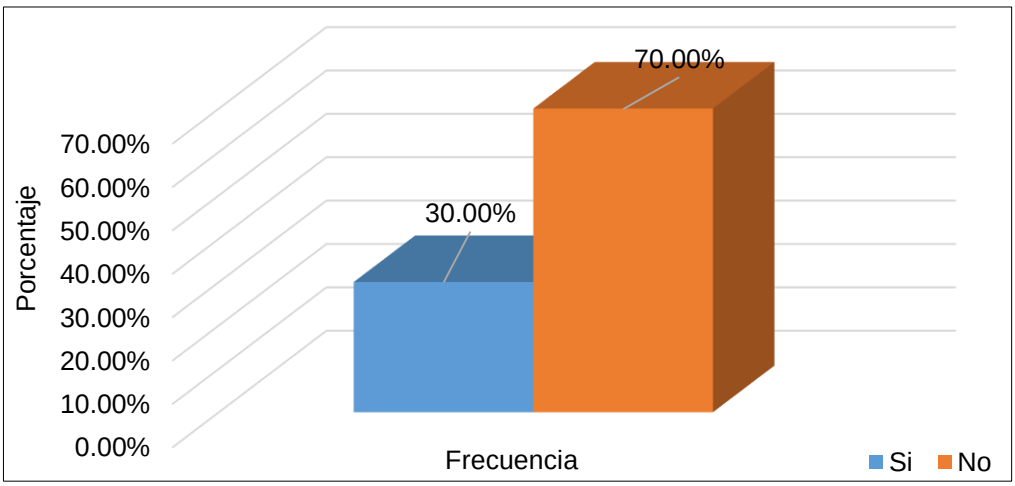
Figura 10
Detención en flagrancia



Interpretación y análisis de resultados

El primer ítem determinó que sólo en el 30.00% de los casos el sujeto fue detenido en flagrancia, ello es evidente por la misma naturaleza y modalidad de la comisión del delito, en el 70.00% no se presentó situación de detención en flagrancia delictiva.

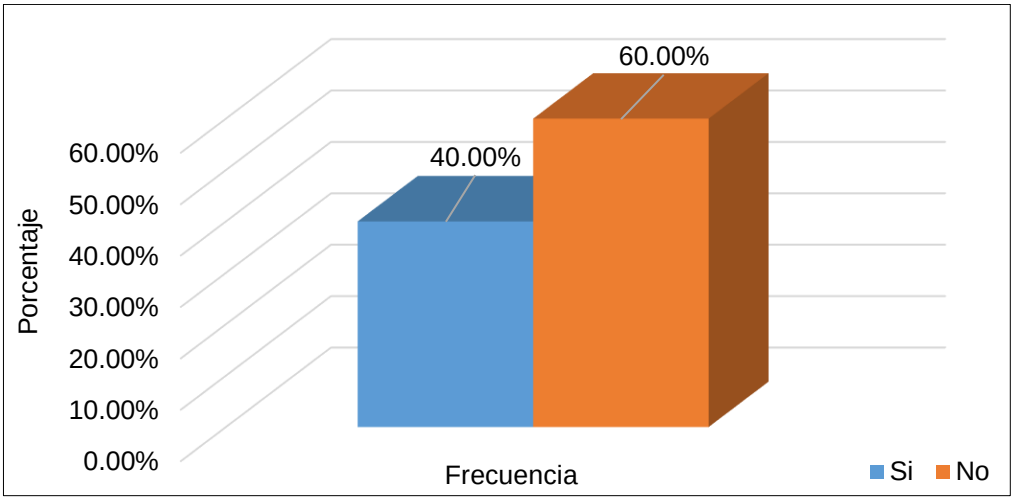
Figura 11
Intervención a sospechosos



Interpretación y análisis de resultados

El segundo ítem fue para conocer en cuántos casos se intervino a sospechosos de delito de fraude informático, de la observación y análisis de casos se tiene que sólo ocurrió en el 30.00% de los casos, mientras que en el 70.00% ello no se presentó.

Figura 12
Recojo de evidencias

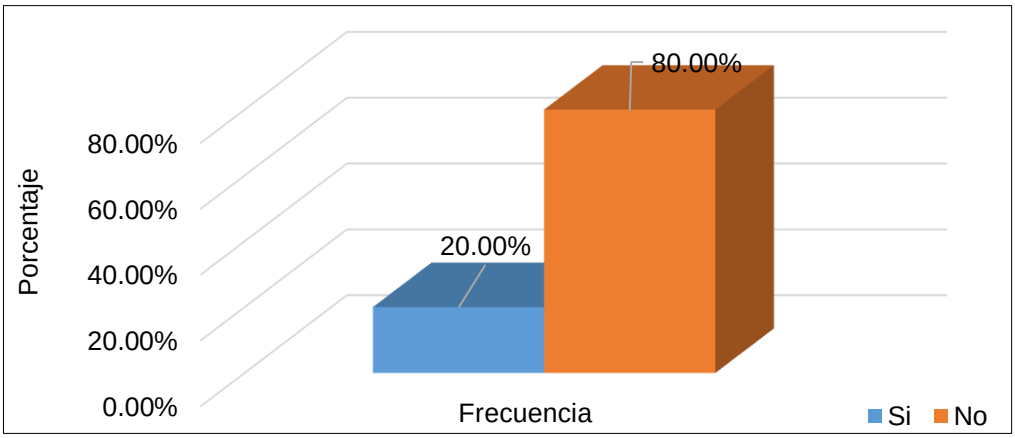


Interpretación y análisis de resultados

El tercer ítem fue para conocer sobre el recojo de evidencias, al respecto se tiene que el 60.00% no se han recogido evidencias y en el 40.00% si se logró ello, de ello se colige que, en los delitos de fraude informático, en muy pocos casos se logra reunir las evidencias que permita una correcta investigación.

2. Dimensión: Actuaciones del fiscal de la investigación

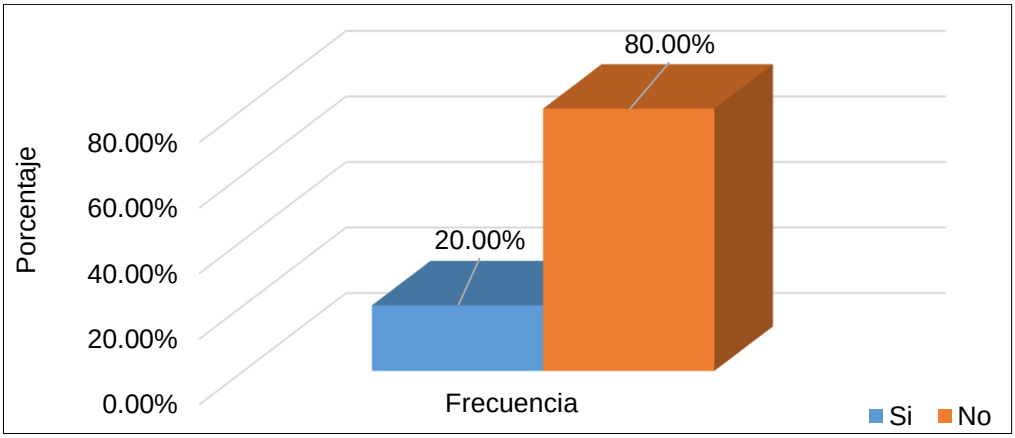
Figura 13
Investigación fiscal suficiente



Interpretación y análisis de resultados

El cuarto ítem fue para conocer la cantidad de casos en los que la investigación fue suficiente, al respecto se tiene que ello únicamente ocurrió en el 20.00% de los casos, mientras que en el 80.00% fue deficiente.

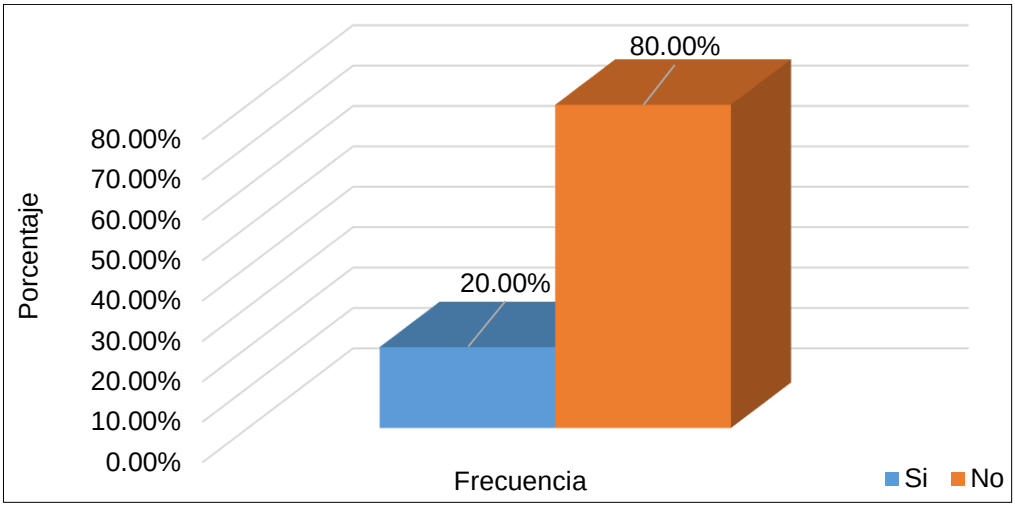
Figura 14
Requerimiento de prisión preventiva



Interpretación y análisis de resultados

El quinto ítem que se observó y analizó fue paca conocer la cantidad de casos en los que se ha requerido la prisión preventiva, al respecto se obtuvo que únicamente en el 20.00% de los casos se requirió la prisión preventiva, mientras que en 80.00% ello no ocurrió.

Figura 15
Acusaciones fiscales

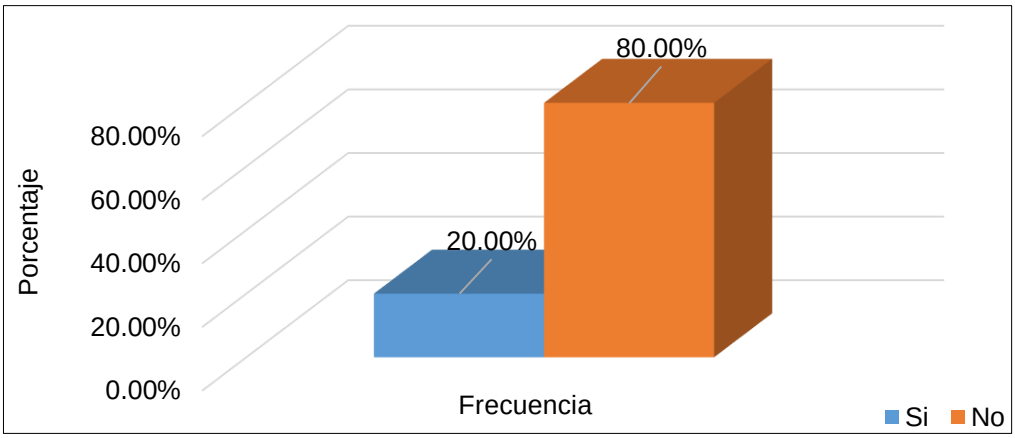


Interpretación y análisis de resultados

El sexto ítem fue para conocer la cantidad de casos en los cuales se han requerido las acusaciones fiscales, al respecto se tiene que únicamente en el 20.00% de ha requerido la acusación fiscal, mientras que en el 80.00% ello no ocurrió.

3. Dimensión: Resoluciones del juez penal

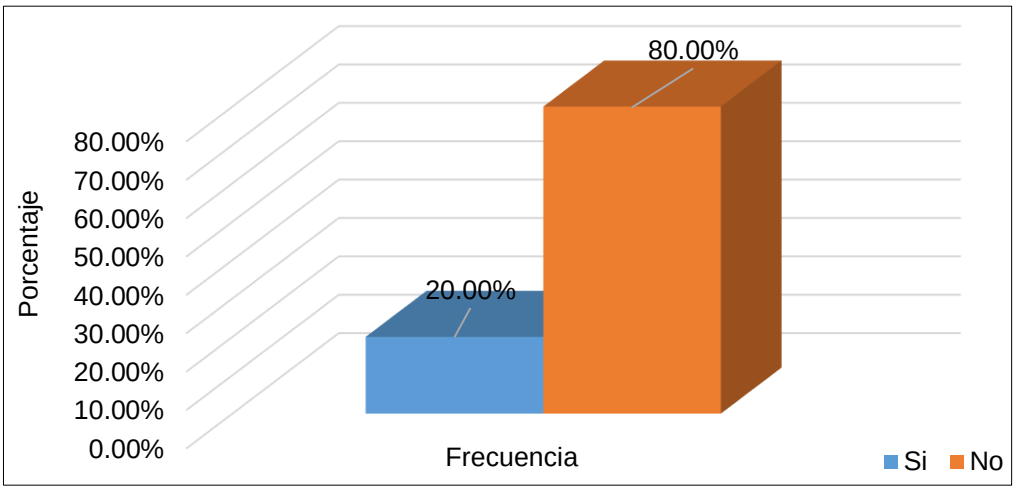
Figura 16
Auto de prisión preventiva



Interpretación y análisis de resultados

El séptimo ítem fue para conocer la cantidad de casos en los cuales el juez ha dictado prisión preventiva y de los resultados se tiene que ello sólo se presenta en el 20.00%, mientras que en el 80.00% ello no ocurrió.

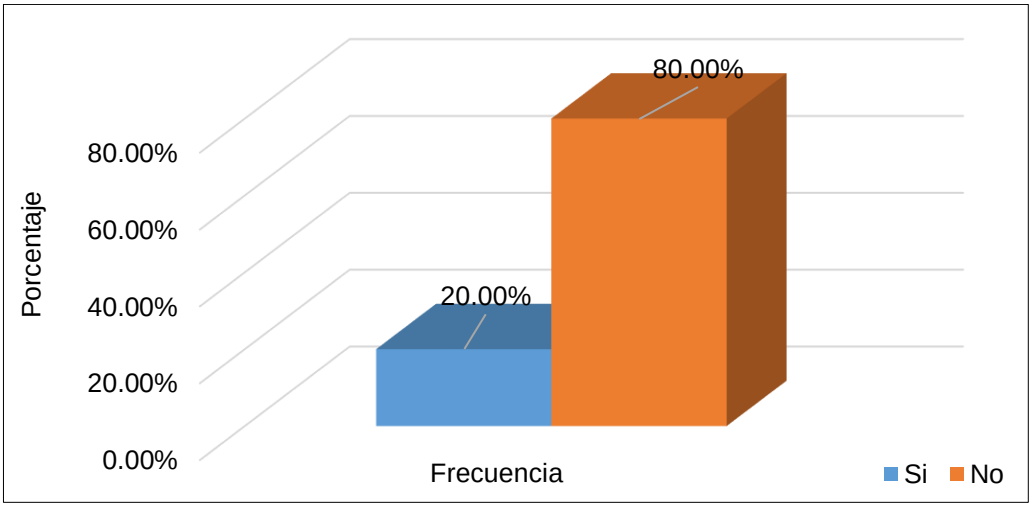
Figura 17
Terminación anticipada



Interpretación y análisis de resultados

El octavo ítem fue para conocer la cantidad de casos en los cuales el juez sentenció por terminación anticipada, de los resultados se desprende que ello ocurrió únicamente en el 20.00% de los casos, mientras que en el 80.00% no se presentó esta situación.

Figura 18
Autos de enjuiciamiento



Interpretación y análisis de resultados

El noveno ítem fue para conocer la cantidad de casos en los cuales el juez ha dictado el auto de enjuiciamiento, al respecto se tiene que ello se presentó únicamente en el 20.00% de los casos, siendo que en el 80.00% ello no ocurrió.

4.2. PRUEBA DE HIPÓTESIS

Se plantearon las hipótesis, luego se halló el coeficiente de correlación de Pearson (r), para lo cual se ha utilizado el software SPSS (versión 26), introduciendo los resultados de cada variable, siendo que, para interpretarlo, se empleó esta tabla:

Tabla 17
Interpretación

Por debajo de .60	Es inaceptable
De .60 a .65	Es indeseable
Entre .65 y .70	Es mínimamente aceptable
De .70 a .80	Es respetable
De .80 a .90	Es muy buena

4.2.1. CONTRASTACIÓN DE HIPÓTESIS GENERAL

La hipótesis general se formuló en el siguiente sentido

HG. La incidencia del delito de fraude informático se relaciona de modo negativo con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023

Ho: $\rho \neq 0$

Ho. La incidencia del delito de fraude informático no se relaciona de modo negativo con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023

Ho: $\rho = 0$

Nivel de significación 0.05

Tabla 18
Comprobación de la hipótesis general

Correlación entre la incidencia del delito de fraude informático y la protección efectiva del ciudadano

Correlaciones			
		Incidencia del delito de fraude informático	**La protección efectiva del ciudadano**
Incidencia del delito de fraude informático	Correlación de Pearson	1	,975**
	Sig. (bilateral)		,004
	N	10	10
La protección efectiva del ciudadano	Correlación de Pearson	,975**	1
	Sig. (bilateral)	,004	
	N	10	10

**. La correlación es significativa en el nivel 0,01 (2 colas).

Análisis e interpretación de resultados

Dado que ρ = 0.004 < 0,05 se rechaza la Ho y se acepta la HG. La incidencia del delito de fraude informático se relaciona de modo negativo con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023, demostrando que se observa una correlación positiva alta con un r = 0,975, lo cual nos permite aseverar, que los resultados de la encuesta nos permiten demostrar que esta incidencia delictiva tiene una relación negativa con la protección efectiva del ciudadano, pues se evidenció que la actuación de los efectivos policiales en relación con el delito de fraude informático no resulta eficaz, del mismo modo las actuaciones del fiscal de la investigación y las del juez penal mediante sus resoluciones no protegen al ciudadano frente a los delitos de fraude informático, a ello debe sumarse también la forma o modo en que se comete este delito, resulta más difícil la detención o intervención de los autores, además del recojo de evidencias lo que acarrea problemas en la investigación y obviamente en el proceso penal; estos resultados también comparados con los resultados de la observación y análisis de casos nos permiten corroborar la hipótesis general, (Tabla 18).

4.2.2. CONTRASTACIÓN DE HIPÓTESIS ESPECÍFICAS

Las hipótesis específicas se plantearon del siguiente modo:

1. Comprobación de la primera hipótesis específica

HE1. La relación de la actuación de la policía nacional del Perú en los delitos de fraude informático no se relaciona eficazmente con la protección efectiva de la víctima en el Distrito Judicial de Huánuco 2022 - 2023

Ho: ρ≠0

Ho. La relación de la actuación de la policía nacional del Perú en los delitos de fraude informático se relaciona eficazmente con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco 2022 - 2023

Ho: ρ=0

Nivel de significación 0.05

Tabla 19
Comprobación de la primera hipótesis específica

Correlación entre la actuación de la policía nacional del Perú y la protección efectiva del ciudadano

Correlaciones

		La actuación de la policía nacional del Perú	Protección efectiva del ciudadano
La actuación de la policía nacional del Perú	Correlación de Pearson	1	,986**
	Sig. (bilateral)		,005
	N	10	10
Protección efectiva del ciudadano	Correlación de Pearson	,986**	1
	Sig. (bilateral)	,005	
	N	10	10

**. La correlación es significativa en el nivel 0,01 (2 colas).

Análisis e interpretación de resultados

Dado que ρ = 0.005 < 0,05 se rechaza la Ho y se acepta la HE1. La relación de la actuación de la policía nacional del Perú en los delitos de fraude informático no se relaciona eficazmente con la protección efectiva de la víctima en el Distrito Judicial de Huánuco 2022 - 2023; demostrando que se observa una correlación positiva alta con un r = 0,986, lo cual nos permite aseverar, la actuación de los efectivos policiales no resulta eficaz para la protección de la víctima este delito, además por la propia naturaleza del mismo; siendo que se han medido tres indicadores que permiten comprobar las hipótesis; evidenciando que nunca o casi nunca se interviene al autor del delito en situación de flagrancia (Tabla 7), que en muy pocas ocasiones se interviene a los sospechosos (Tabla 8), además de la falta de especialización policial en el recojo de evidencias en este delitos (Tabla 9).

2. Comprobación de la segunda hipótesis específica

HE2. Las actuaciones del fiscal en la investigación por el delito de fraude informático no protegen de forma efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023

Ho: ρ≠0

Ho. Las actuaciones del fiscal en la investigación por el delito de fraude informático protegen de forma efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023

Ho: ρ=0

Nivel de significación 0.05

Tabla 20
Comprobación de la segunda hipótesis específica

Correlación entre las actuaciones del fiscal en la investigación por delito de fraude informático y la protección efectiva del ciudadano

Correlaciones			
		Las actuaciones del fiscal en la investigación del delito de fraude informático	**La protección efectiva del ciudadano**
Las actuaciones del fiscal en la investigación del delito de fraude informático	Correlación de Pearson	1	,988**
	Sig. (bilateral)		,006
	N	10	10
La protección efectiva del ciudadano	Correlación de Pearson	,988**	1
	Sig. (bilateral)	,006	
	N	10	10

**. La correlación es significativa en el nivel 0,01 (2 colas).

Análisis e interpretación de resultados

Dado que ρ = 0.006 < 0,05 se rechaza la Ho y se acepta la HE2. Las actuaciones del fiscal en la investigación por el delito de fraude informático no protegen de forma efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023, demostrando que se observa una correlación positiva alta con un r = 0,988, lo cual nos permite aseverar que, se ha demostrado que las actuaciones del fiscal que se encarga de la investigación de los delitos de fraude informático no protegen de forma efectiva al ciudadano, al respecto se han medido tres indicadores evidenciando que en muy poco casos, estas casi siempre son adecuadas, (Tabla 10), además frente a una inadecuada investigación casi nunca requiere la prisión preventiva, (Tabla 11) y del mismo modo casi nunca presenta en requerimiento de acusación, (Tabla 12)

3. Comprobación de la tercera hipótesis específica

HE3. Las resoluciones dictadas por los jueces en los delitos de fraude informático no protegen de modo efectivo del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023

Ho: ρ=0

Ho. Las resoluciones dictadas por los jueces en los delitos de fraude informático protegen de modo efectivo del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023

Ho: ρ≠0

Nivel de significación 0.05

Tabla 21

Comprobación de la tercera hipótesis específica

Correlación entre las resoluciones dictadas por los jueces en los delitos de fraude informático y la protección de modo efectivo al ciudadano

Correlaciones			
		Las resoluciones dictadas por los jueces en los delitos de fraude informático	**Protección de modo efectivo al ciudadano**
Las resoluciones dictadas por los jueces en los delitos de fraude informático	Correlación de Pearson	1	,896**
	Sig. (bilateral)		,008
	N	10	10
Protección de modo efectivo al ciudadano	Correlación de Pearson	,896**	1
	Sig. (bilateral)	,008	
	N	10	10

**. La correlación es significativa en el nivel 0,01 (2 colas).

Análisis e interpretación de resultados

Dado que ρ = 0.008 < 0,05 se rechaza la Ho y se acepta la HE3. Las resoluciones dictadas por los jueces en los delitos de fraude informático no protegen de modo efectivo del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023, demostrando que se observa una correlación positiva alta con un r = 0,896, lo cual nos permite aseverar que, se ha demostrado que las resoluciones judiciales en los casos por delito de fraude informático tampoco protegen de modo efectivo al ciudadano, siendo que han medido tres indicadores, de lo que se colige que casi nunca se dictan prisiones preventivas, ello obviamente porque el fiscal no lo requiere o porque los requerimientos no contienen todos los presupuestos establecidos, (Tabla 13), del mismo modo casi nunca se arriban a terminaciones anticipadas, ello obviamente porque las investigaciones son inadecuadas ya que no se cuentan con todos los elementos de convicción y / o evidencias, (Tabla 14), y del mismo modo casi nunca se dicta el auto de enjuiciamiento, porque con muy pocos los casos en los cuales hay requerimiento acusatorio, (Tabla 15).

CAPÍTULO V
DISCUSIÓN DE RESULTADOS

5.1. DISCUSIÓN DE RESULTADOS

5.1.1. DISCUSIÓN DE RESULTADOS A PARTIR DE LOS ANTECEDENTES

Es evidente, que desde las dos décadas de este siglo, el mundo se ha visto envuelto en una revolución tecnológica e informática, que ha optimizado las relaciones sociales, económicas y laborales; pero también ha surgido un nuevo contexto de delitos, llamados delitos informáticos, en los cuales los sujetos activos o criminales se valen de ello, además del anonimato, la rapidez e incluso la posibilidad de cometer delitos desde servidores o software instalados en lugares lejanos y distantes para cometer sus delitos, delitos que no se cometen solo en el mundo objetivo sino a través de la realidad virtual, ello produce una serie de efectos y desafíos que nuestros marcos jurídicos no pueden contener, (Echevarría, 2020, p. 121)

Los delitos informáticos son variados, así como variadas resultan ser las posibilidades que las relaciones no solo personales, empresariales institucionales y estatales pueden servirse de estas nuevas tecnologías, de este modo la ciber delincuencia debe ser enfrentada a través de convenios internacionales como el Tratado de Budapest, además de una policía internacional, es decir, el trabajo y acciones conjuntas y coordinadas de los países, pues como ya se ha indicado el delito de puede cometer en un lugar distinto al de donde se generan sus efectos jurídicos, (Peña, 2023, p. 352)

En nuestro país el índice de la ciberdelincuencia es alto, y si bien se cuenta con la Ley N. 30096, que tipifica una serie de conductas delictivas, entre ellas el fraude informático, no es menos cierto que en el tema de la investigación se presentan una serie desafíos a las que nos

enfrentamos, sobre todo en la lucha contra este delitos, pues no se cuenta con una policía ni fiscalía especializada, ni tampoco con medios tecnológicos de punta que permitan una adecuada investigación, requiriendo siempre del apoyo internacional, lo que demanda tiempo en las investigaciones, ello también se evidenció de los resultados arribados en la presente tesis, (Villanueva, 2023, p. 116)

Uno de los delitos más frecuentes dentro del espectro de la ciberdelincuencia corresponde a los fraudes informáticos y la clonación de tarjetas bancarias, y a pesar de la tipificación de los delitos mediante la Ley N. 30096 y su modificatoria, es evidente como ha quedado demostrado en la presente investigación, el principal problema evidenciado corresponde a la etapa de la investigación, pues la DIAT que es la Dirección Policial de Alta Tecnología puesto que no cuenta con equipo de peritos especialistas en este tipo de criminalidad, aunado a ello la fiscalía tampoco es especializada en esta forma de criminalidad, por lo que se presentan situaciones problemáticas para identificar al autor, lo cual se hace posible debido a las técnicas de encriptación que ocultan la identidad del autor, así como al uso de sistemas informáticos que facilitan el accionar de los ciberdelincuentes y lógicamente ser juzgados y condenados. (Carbajal, 2022, p. 225)

Los resultados que permitieron la comprobación de hipótesis se evidenciaron, además, en una tesis de esta ciudad, en la cual, si bien trata de delitos informáticos entre ellos el fraude informático, muchos de estos casos se archivan porque no se cuentan con los recursos humanos especializados y medios logísticos suficientes para una adecuada investigación dejando en estado de vulneración a las víctimas, (Romero, 2021, p. 152)

5.1.2. DISCUSIÓN DE RESULTADOS DESDE LAS BASES TEÓRICAS

La presente tesis ha investigado sobre el delito de fraude informático, siendo este un delito que se encuentra dentro de la gama de delito informáticos o ciberdelitos, que es modo nuevo de criminalidad que se realiza dentro del amplio territorio del ciberespacio, el mismo que genera una serie de problemas y desafíos para la seguridad, la privacidad y la estabilidad económica, que corresponde una amenaza constante para individuos, empresas, instituciones y el propio Estado, (López, 2024, p. 130); se entiende como fraude informático a aquellas estafas realizadas mediante el internet, como la venta de productos falsificados o inexistentes, o la suplantación de identidad para obtener beneficios ilícitos, (Ribón, 2024, p. 209)., en decir, el uso de medios digitales para engañar y defraudar a las personas y empresas con la finalidad de apoderarse del patrimonio de éstas, específicamente en dinero, (Espinoza, 2023, p. 190), que obviamente genera un fuerte impacto en las personas, la sociedad por las consecuencias económicas, (Camacho, 2108, p. 137).

Siendo que este modalidad delictiva es muy difícil establecer el lugar de su comisión y los efectos que produce, pues éstos pueden multiplicarse en distintos lugares no solo del país, sino del planeta, es importante la Cooperación Internacional, es decir, un colaboración estrecha entre países y agencias de aplicación de la ley para investigar y combatir el ciberdelito a nivel global, lo que evidencia la necesidad de equiparar los protocolos y la estrecha colaboración de información, que devienen en fundamentales, pero también es necesario que se fortalezca la seguridad cibernética, tanto a nivel empresarial, institucional y personal, como firewalls, cifrado de datos, importante es un marco jurídico que aborde este delito, (Herrera, 2024, 207); pero ello no basta, es decir sin desconocer la importancia del Tratado de Budapest y los protocolos internacionales, ya que se requiere que dentro del propio país se disponga de medios logísticos y recursos humanos

que hagan frente a este delito, lo que no viene ocurriendo, pues a pesar que los ciudadanos emplean y utilizan los sistemas digitales para realizar sus transacciones para adquirir bienes y servicios, así como realizar sus actividades bancarias, cada vez es menos las situaciones en que las personas tienen dinero en metálico, sino que habilitan sus cuentas bancarias a sus correos electrónicos y teléfono celulares, no se cuenta una policía ni fiscalía especializada, tampoco con los medios suficientes para la investigación, (Villanueva, 2023, p. 154), lo que deriva que no hay una adecuada protección al ciudadano frente a la comisión del delito de fraude informático, (Camacho, 2018, p. 213)

5.1.3. DISCUSIÓN DE RESULTADOS DESDE LA COMPROBACIÓN DE HIPÓTESIS

Los resultados obtenidos a partir de la encuesta a la muestra, los mismos que han sido contrastados con los resultados de la observación y análisis de casos, han permitido la comprobación de las hipótesis, pues se ha encontrado una correlación positiva alta entre las variables de estudio, logrando establecer que en el caso de la hipótesis general existe un coeficiente de correlación de Pearson de 0,975, por ende, se logró demostrar que la que esta incidencia delictiva del delito de fraude informático tiene una relación negativa con la protección efectiva del ciudadano, ello a partir de las deficiencias de la actuación de los efectivos policiales, las actuaciones del fiscal de la investigación y las del juez penal mediante sus resoluciones, no protegen eficazmente al ciudadano.

En este orden de ideas, respecto a la primera hipótesis específica se halló un coeficiente de correlación de Pearson positivo alto de 0,986 logrando demostrar que la actuación de la policía nacional del Perú en los delitos de fraude informático no protege de manera efectiva la víctima, puesto que nunca o casi nunca se interviene al autor del delito en situación de flagrancia, en muy pocas ocasiones se interviene a los

sospechosos y la se evidencia falta de especialización policial en el recojo de evidencias en este delito.

Además, los resultados arribados nos han permitido hallar un coeficiente de correlación de Pearson positivo alto de 0,988 en la segunda hipótesis específica, lo nos permitió demostrar que las actuaciones del fiscal en la investigación por el delito de fraude informático no protegen de forma efectiva del ciudadano, puesto en muy pocos casos, estas casi siempre son adecuadas y logran su finalidad; lo que genera que casi nunca se requiera la prisión preventiva, así como el requerimiento de acusación.

Los resultados también no han permitido hallar un coeficiente de correlación de Pearson positivo alto, de 0,896, logrando demostrar la tercera hipótesis específica, que las resoluciones judiciales en los casos por delito de fraude informático tampoco protegen de modo efectivo al ciudadano, siendo que han medido tres indicadores, de lo que se colige que casi nunca se dictan prisiones preventivas, ello obviamente porque el fiscal no lo requiere o porque los requerimientos no contienen todos los presupuestos establecidos, del mismo modo casi nunca se arriban a terminaciones anticipadas, ello obviamente porque las investigaciones son inadecuadas ya que no se cuentan con todos los elementos de convicción y / o evidencias y casi nunca se dicta el auto de enjuiciamiento, porque con muy pocos los casos en los cuales hay requerimiento acusatorio.

CONCLUSIONES

Primera

Se llegó a describir que la incidencia del delito de fraude informático se relaciona de modo negativo con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023, porque se han verificado deficiencias de la actuación de los efectivos policiales, en las actuaciones fiscal de la investigación y lo que ha repercutido en las resoluciones judiciales.

Segunda

Se logró determinar que la actuación de la policía nacional del Perú en los delitos de fraude informático no se relaciona eficazmente con la protección efectiva de la víctima en el Distrito Judicial de Huánuco 2022 – 2023, puesto que nunca o casi nunca se interviene al autor del delito en situación de flagrancia, en muy pocas ocasiones se interviene a los sospechosos y la se evidencia falta de especialización policial en el recojo de evidencias en este delito.

Tercera

Se logró establecer que las actuaciones del fiscal en la investigación por el delito de fraude informático no protegen de forma efectiva a la víctima en el Distrito Judicial de Huánuco, 2022 – 2023, pues en muy pocos casos, estas casi siempre son adecuadas y logran su finalidad; lo que genera que casi nunca se requiera la prisión preventiva, así como el requerimiento de acusación.

Cuarta

Se explica que el modo que las resoluciones dictadas por los jueces en los delitos de fraude informático no protegen de modo efectivo a la víctima en el Distrito Judicial de Huánuco, 2022 – 2023, ya que casi nunca se dictan prisiones preventivas, casi nunca se arriban a terminaciones anticipadas, y casi nunca se dicta el auto de enjuiciamiento, porque con muy pocos los casos en los cuales hay requerimiento acusatorio.

RECOMENDACIONES

Primera.

Se recomienda al Director de la Policía Nacional del Perú, de la Región Policial de Huánuco, al Presidente de la Junta de Fiscales de Huánuco y al Presidente de la Corte Superior de Justicia de Huánuco, trabajar de modo adecuado y coordinado frente a la incidencia de delitos de fraude informático a efectos de proteger de modo eficaz al ciudadano, porque se ha evidenciado deficiencias en la actuación de los efectivos policiales, de los fiscales y de los jueces penales.

Segunda

Se recomienda al Director de la Policía Nacional del Perú, de la Región Policial de Huánuco, actuar de manera adecuada y coordinada con otras regiones y el extranjero, frente a la flagrancia delictiva de los delitos informáticos, además realizar una adecuada intervención de sospechosos y principalmente solicitar el presupuesto para contar los recursos tecnológicos e informáticos de punta, que permita un adecuada investigación, recolección de evidencias, además de requerir para ello de personal especializado de criminalística informática.

Tercera

Se recomienda al presidente de la Junta de Fiscales de Huánuco, exhortar a los fiscales especializados en delitos informáticos, que se encuentran debidamente preparados mediante cursos y tallares, a efectos de realizar una adecuada investigación que le permita el esclarecimiento de los hechos, realizar actos de investigación a efectos de solicitar las prisiones preventivas y requerimientos acusatorios.

Cuarta

Se recomienda al Presidente de la Corte Superior de Justicia de Huánuco, que frente a los requerimientos fiscales de delitos de fraude informático realizar un análisis adecuado del caso a efectos que frente a ellos pueda pronunciarse por la prisión preventiva, terminaciones anticipadas y autos de enjuiciamiento.

REFERENCIAS BIBLIOGRÁFICAS

Camacho, L. (2108). *El delito informático. Un análisis en profundidad mayor riesgo con que se enfrenta la sociedad indformatizada*. Madrid: Aranzadi.

Carbajal, M. (2022). *Las fiscalías especializadas en delitos informáticos como mecanismo para la lucha contra el ciber crimen. Lima - Perú:* Tesis para optar el grado de maestra en ciencias penales por la Universidad San Martín de Porras. Obtenido de https://repositorio.usmp.edu.pe/bitstream/handle/20.500.12727/11398/carbajal_cm.pdf?sequence=1&isAllowed=y

Castillo, Z. (2020). *Metodología de la investigación científica.* Huánuco: Ed. San Marcos.

Cussianovich, A., Tello, J., & Sotelo, M. (23 de 08 de 2007). www.pj.gob.pe. Obtenido de http://file://C:/Users/FN/Downloads/violenciaintrafamiliar1107708.pdf

Echevarría, G. (2015). *Los delitos informáticos y el derecho constitucional a la seguridad pública. Ambato - Ecuador*: Tesis para optar el grado de maestra en Derecho Penal por la Universidad Técnica de Ambato. Obtenido de https://repositorio.uta.edu.ec/jspui/handle/123456789/10034

Espinoza, V. (2023). *Cibercriminalidad y delitos informáticos.* Lima: Jurista Editores.

Fontena, C., & Gatica, A. (25 de 09 de 2015). www.ubioubio.cl. Obtenido de http://cps/ponencia/doc/p10.4/htlm

Gutiérrez, E. (2021). Delitos informáticos. Paso a paso. Bogotá : Colex.

Herrera, S. (2024). *Delitos informáticos*. Análisis dogmático y comentarios de la ley. Madrid: Tirant Lo Blanch.

Lancho - Barrantes, B., & Cantú - Ortiz, F. (2020). *Midiendo la influencia de los factores sociales en la investigación científica*. Investigación Biliocotelógica ISSN 2448 - 8321, Ciudad de México. Obtenido de https://www.scielo.org.mx/scielo.php?pid=S0187-358X2020000400061&script=sci_abstract

López, J. (2024). C*iberdelincuencia*. Espacio delictivo y participación. Navarra: Aranzadi.

Martínez, R. (2020). *El secreto detrás de una tesis.* Lima: Ed. Rosario Martínez.

Navagarces, A. (2022). *Delitos informáticos*. 5ta. Edición. Ciudad de México: Porrúa.

Peña, M. (2023). *Delitos cibernéticos. Bogotá - Colombia: Tesis para optar el grado de maestro en Derecho Penal por la Universidad Libre de Colombia.* Obtenido de https://repository.unilibre.edu.co/bitstream/handle/10901/24774/TESIS%20VERSION%20APROBADA.pdf?sequence=1&isAllowed=y

Ribón, E. (2024). *Fraudes bancarios y defensa del afectado: nuevas tendencias defraudatorias*. Valencia: Tirant Lo Blanch.

Rivera, H. (2022). *Los delitos informáticos y su incidencia en la gestión de las instituciones del Estado del Dsitrito de Huánuco, 2017. Huánuco - Perú*: Tesis para optar el grado de Doctora en Derecho por la Universidad Nacional Hermilio Valdizán. Obtenido de file:///C:/Users/Asus/Downloads/TDr.D00101R68%20(1).pdf

Romero, H., Palacios, J., & Ñaupas , H. (2020). *Metodología de la investigación jurídica*. Una brújula para investigar y redactar la tesis. Lima: Grijley.

Romero, M. (2017). *Delitos informáticos cometidos a través de las redes sociales y su tratamiento en el Ministerio Público en la ciudad de Huánuco, 2016. Huánuco:* Tesis para optar el título de abogada por la

Universidad de Huánuco. Obtenido de http://repositorio.udh.edu.pe/bitstream/handle/123456789/331/T_047_%2025858529_T.pdf?sequence=1&isAllowed=y

Valencia, J. (2022). *Los delitos informáticos*. Bogotá: Leyer.

Vega, J., & Arevalo, M. (2022). *Ciberdelitos*. Análisis de sistema penal. Lima: Iustitia.

Villanueva, J. (2023). *Ley de los delitos informáticos N. 30096 y su influencia en la población de Chiclayo en tiempos del COVID 19. Chiclayo - Perú:* Tesis para optar el título de abogado por la Universidad Señor de Sipán. Obtenido de https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/10627/Villanueva%20Calderon%20Juan%20Amilcar.pdf?sequence=1&isAllowed=y

Zevallos, U. (2020). M*etodología de la investigación jurídica*. Huánuco: Ed. San Marcos.

COMO CITAR ESTE TRABAJO DE INVESTIGACIÓN

Herrera Figueroa, G. (2026). *La incidencia del delito de fraude informático y la protección efectiva del ciudadano, distrito judicial de Huánuco, 2022 - 2023* [Tesis de pregrado, Universidad de Huánuco]. Repositorio Institucional UDH. http://…

ANEXOS

ANEXO 1
MATRIZ DE CONSISTENCIA

LA INCIDENCIA DEL DELITO DE FRAUDE INFORMÁTICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023

Problema	Objetivos	Hipótesis	Variables	Dimensiones	Indicadores
Problema Principal	**Objetivo General**	**Hipótesis General**			
¿De qué modo la incidencia del delito de fraude informático se relaciona con la protección efectiva del ciudadano, en el Distrito Judicial de Huánuco, 2022 - 2023?	Describir el modo en que la incidencia del delito de fraude informático se relaciona con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023	**HG.** La incidencia del delito de fraude informático se relaciona de modo negativo con la protección efectiva de la víctima en el Distrito Judicial de Huánuco, 2022 – 2023 **Ho.** La incidencia del delito de fraude informático no se relaciona de modo negativo con la protección efectiva de la víctima en el Distrito Judicial de Huánuco, 2022 – 2023	**VI. Variable Independiente** La incidencia del delito de fraude informático	Actuación de la Policía Nacional del Perú.	Detención en flagrancia delictiva Intervenciones a sospechosos Recojo de evidencias
Problemas Específicos	**Objetivos Específicos**	**Hipótesis Específicas**		Actuaciones del fiscal de la investigación	Investigaciones fiscales Requerimiento de prisión preventiva Acusaciones fiscales
PE1. ¿Cómo se relaciona la actuación de la policía nacional del Perú en los delitos de fraude informático con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco 2022 - 2023?	**OE1.** Determinar la relación de la actuación de la policía nacional del Perú en los delitos de fraude informático y la protección efectiva del ciudadano en el Distrito Judicial de Huánuco 2022 - 2023	**HE1**. La relación de la actuación de la policía nacional del Perú en los delitos de fraude informático no se relaciona eficazmente con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco 2022 - 2023 **Ho.** La relación de la actuación de la policía nacional del Perú en los delitos de fraude informático se relaciona eficazmente con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco 2022 - 2023	**VD. Variable Dependiente** Protección efectiva del ciudadano	Resoluciones del juez penal	Dictó prisión preventiva Arribo a terminaciones

Problema	Objetivos	Hipótesis	Variables	Dimensiones	Indicadores
PE2. ¿De qué forma las actuaciones del fiscal en la investigación por el delito de fraude informático se relaciona con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023?	**OE2.** Establecer la forma en que las actuaciones del fiscal en la investigación por el delito de fraude informático se relacionan con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023	**HE2**. Las actuaciones del fiscal en la investigación por el delito de fraude informático no protegen de forma efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023 **Ho.** Las actuaciones del fiscal en la investigación por el delito de fraude informático protegen de forma efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023			anticipadas Se dictó el auto de enjuiciamiento
PE3. ¿De qué modo las resoluciones dictadas por los jueces en los delitos de fraude informático se relacionan con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023?	**OE3.** Explicar el modo que las resoluciones dictadas por los jueces en los delitos de fraude informático se relacionan con la protección efectiva del ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023	**HE3.** Las resoluciones dictadas por los jueces en los delitos de fraude informático no protegen de modo efectivo al ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023 **Ho.** Las resoluciones dictadas por los jueces en los delitos de fraude informático protegen de modo efectivo al ciudadano en el Distrito Judicial de Huánuco, 2022 – 2023			

ANEXO 2
CUESTIONARIO

Sr. (a) Encuestado (a)

Se le solicita que responda el presente cuestionario para efectos de la investigación titulada: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMÁTICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023. Responsable: Bach. Grecia Isabel Herrera Figueroa, para tal efecto se solicita que responda las siguientes preguntas de acuerdo a las alternativas:

5	4	3	2	1
Siempre	Casi siempre	Indiferente	Casi nunca	Nunca

CUESTIONARIO				VALORES				
VARIABLE	**DIMENSIONES**	**INDICADORES**	**ÍTEMS**	**5**	**4**	**3**	**2**	**1**
Vx. La incidencia del delito de fraude informático	Actuación de la Policía Nacional del Perú	Detención en flagrancia delictiva	¿La Policía Nacional del Perú detuvo en flagrancia al autor y partícipes del delito?					
		Intervenciones a sospechosos	¿La Policía Nacional del Perú intervino a sospechosos del delito?					
		Recojo de evidencias	¿La Policía Nacional del Perú cuenta con la especialización en el recojo de evidencias del delito de fraude informático?					
		Investigaciones fiscales	¿La investigación fiscal fue adecuada?					
Vy. Protección efectiva de la víctima	Actuaciones del fiscal de la investigación	Requerimientos de prisión preventiva	¿El fiscal requirió la prisión preventiva del autor y / o partícipes?					
		Acusaciones fiscales	¿El fiscal requirió la acusación fiscal?					
		Dictó prisión preventiva	¿El juez dictó prisión preventiva al autor y / o partícipes?					
	Resoluciones del juez penal	Arribó a terminaciones anticipadas	¿Se arribaron a terminaciones anticipadas con el resarcimiento a la víctima?					
		Dictó auto de enjuiciamiento	¿El juez emitió el auto de enjuiciamiento?					

ANEXO 3
FICHA DE MATRIZ DE ANALISIS DE CASOS

Sr. (a) Encuestado (a)

Título: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMÁTICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023.

Responsable: Bach. Grecia Isabel Herrera Figueroa, para tal efecto se solicita que responda las siguientes preguntas de acuerdo a las alternativas

N.	N. Carpeta Fiscal	Actuaciones de la Policía Nacional del Perú			Actuaciones del Fiscal en la investigación			Resoluciones del Juez Penal		
		Detención en flagrancia	Intervención a sospechosos	Recojo de evidencias	Investigación fiscal suficiente	Requerimiento de prisión preventiva	Acusaciones fiscales	Auto de prisión preventiva	Terminación anticipada	Requerimiento acusatorio
1										
2										
3										
4										
5										
6										
7										
8										
9										
10										
Total										

ANEXO 4
CONSENTIMIENTO INFORMADO

Sr. (a) Encuestado (a)

Ud. ha sido seleccionado como muestra para ser encuestado, para fines eminentemente académicos, para el desarrollo de la investigación titulada Título: Título: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMÁTICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023, a cargo de la Bachiller Grecia Isabel Herrera Figueroa.

Se le informa que los datos que se obtengan de la presente encuesta sólo serán utilizados para los fines de la investigación, además el investigador va a guardar absoluta reserva de su identidad, precisando también que no se va a pagar suma alguna por su participación.

En caso de aceptar, marque con un aspa donde corresponde.

De antemano el tesista agradece por su atención.

Firma de la muestra

ANEXO 5
VALIDACIÓN DE INSTRUMENTOS

VALIDACIÓN DE INSTRUMENTO – CUESTIONARIO

Nombre del Experto: Dr. DAVID BERAUN SÁNCHEZ **Especialidad:** Derecho - Investigación

Título: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMÁTICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023.

Responsable: Bach. Grecia Isabel Herrera Figueroa

Instrucciones: Calificar con 1, 2, 3 o 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad.

CRITERIOS	INDICADORES	INACEPTABLE					MÍNIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1.- CLARIDAD	Está formulado con un lenguaje comprensible													X
2.- OBJETIVIDAD	Está adecuado a las leyes y principios científicos													X
3.- ACTUALIDAD	Está adecuado a los objetivos y 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 y supuestos jurídicos													X
9.- METODOLOGÍA	La estructura responde a una metodología y diseño aplicados para verificar los supuestos jurídicos.													X
10.- PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al método científico													X

¿Hay alguna dimensión o ítem que no fue evaluada? Sí ( ) No (x) **Decisión del Experto**: El instrumento debe ser: aplicado (x) no aplicado ( ) mejorado ( )

Dr. DAVID BERAUN SANCHEZ
DNI 22474797

VALIDACIÓN DE INSTRUMENTO – MATRIZ DE ANÁLISIS

Nombre del Experto: Dr. DAVID BERAUN SÁNCHEZ **Especialidad:** Derecho - Investigación

Título: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMÁTICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023.

Responsable: Bach. Grecia Isabel Herrera Figueroa

Instrucciones: Calificar con 1, 2, 3 o 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad.

CRITERIOS	INDICADORES	INACEPTABLE						MÍNIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1.- CLARIDAD	Está formulado con un lenguaje comprensible													X
2.- OBJETIVIDAD	Está adecuado a las leyes y principios científicos													X
3.- ACTUALIDAD	Está adecuado a los objetivos y 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 y supuestos jurídicos													X
9.- METODOLOGÍA	La estructura responde a una metodología y diseño aplicados para verificar los supuestos jurídicos.													X
10.- PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al método científico													X

¿Hay alguna dimensión o ítem que no fue evaluada? Sí ( ) No (x) **Decisión del Experto**: El instrumento debe ser: aplicado (x) no aplicado ( ) mejorado ( )

Dr. DAVID BERAUN SANCHEZ
DNI 22474797

VALIDACIÓN DE INSTRUMENTO – CUESTIONARIO

Nombre del Experto: Mg. HENRI SOTO PEREZ **Especialidad:** Derecho - Investigación

Título: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMÁTICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023.

Responsable: Bach. Grecia Isabel Herrera Figueroa

Instrucciones: Calificar con 1, 2, 3 o 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad.

CRITERIOS	INDICADORES	INACEPTABLE						MÍNIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1.- CLARIDAD	Está formulado con un lenguaje comprensible													X
2.- OBJETIVIDAD	Está adecuado a las leyes y principios científicos													X
3.- ACTUALIDAD	Está adecuado a los objetivos y 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 y supuestos jurídicos													X
9.- METODOLOGÍA	La estructura responde a una metodología y diseño aplicados para verificar los supuestos jurídicos.													X
10.- PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al método científico													X

¿Hay alguna dimensión o ítem que no fue evaluada? Sí ( ) No (x) **Decisión del Experto**: El instrumento debe ser: aplicado (x) no aplicado ( ) mejorado ( )

VALIDACIÓN DE INSTRUMENTO – MATRIZ DE ANÁLISIS

Nombre del Experto: Mg. HENRI SOTO PEREZ **Especialidad: Derecho - Investigación**

Título: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMÁTICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023.

Responsable: Bach. Grecia Isabel Herrera Figueroa

Instrucciones: Calificar con 1, 2, 3 o 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad.

CRITERIOS	INDICADORES	INACEPTABLE						MÍNIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1.- CLARIDAD	Está formulado con un lenguaje comprensible													X
2.- OBJETIVIDAD	Está adecuado a las leyes y principios científicos													X
3.- ACTUALIDAD	Está adecuado a los objetivos y 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 y supuestos jurídicos													X
9.- METODOLOGÍA	La estructura responde a una metodología y diseño aplicados para verificar los supuestos jurídicos.													X
10.- PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al método científico													X

¿Hay alguna dimensión o ítem que no fue evaluada? Sí ( ) No (x) **Decisión del Experto**: El instrumento debe ser: aplicado (x) no aplicado ( ) mejorado ( )

VALIDACIÓN DE INSTRUMENTO – CUESTIONARIO

Nombre del Experto: Mg. ZÓSIMO CASTILLO LOBATON **Especialidad:** Investigación

Título: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMÁTICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023.

Responsable: Bach. Grecia Isabel Herrera Figueroa

Instrucciones: Calificar con 1, 2, 3 o 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad.

CRITERIOS	INDICADORES	INACEPTABLE						MÍNIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1.- CLARIDAD	Está formulado con un lenguaje comprensible													X
2.- OBJETIVIDAD	Está adecuado a las leyes y principios científicos													X
3.- ACTUALIDAD	Está adecuado a los objetivos y 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 y supuestos jurídicos													X
9.- METODOLOGÍA	La estructura responde a una metodología y diseño aplicados para verificar los supuestos jurídicos.													X
10.- PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al método científico													X

¿Hay alguna dimensión o ítem que no fue evaluada? Sí ( ) No (x) **Decisión del Experto**: El instrumento debe ser: aplicado (x) no aplicado ( ) mejorado ( )

VALIDACIÓN DE INSTRUMENTO – MATRIZ DE ANÁLISIS

Nombre del Experto: Mg. ZÓSIMO CASTILLO LOBATON **Especialidad: Investigación**

Título: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMÁTICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023.

Responsable: Bach. Grecia Isabel Herrera Figueroa

Instrucciones: Calificar con 1, 2, 3 o 4 cada ítem respecto a los criterios de relevancia, coherencia, suficiencia y claridad.

CRITERIOS	INDICADORES	INACEPTABLE						MÍNIMAMENTE ACEPTABLE			ACEPTABLE			
		40	45	50	55	60	65	70	75	80	85	90	95	100
1.- CLARIDAD	Está formulado con un lenguaje comprensible													X
2.- OBJETIVIDAD	Está adecuado a las leyes y principios científicos													X
3.- ACTUALIDAD	Está adecuado a los objetivos y 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 y supuestos jurídicos													X
9.- METODOLOGÍA	La estructura responde a una metodología y diseño aplicados para verificar los supuestos jurídicos.													X
10.- PERTINENCIA	El instrumento muestra la relación entre los componentes de la investigación y su adecuación al método científico													X

¿Hay alguna dimensión o ítem que no fue evaluada? Sí ( ) No (x) **Decisión del Experto**: El instrumento debe ser: aplicado (x) no aplicado ( ) mejorado ( )

ANEXO 6
INSTRUMENTOS APLICADOS

Anexo 2. Cuestionario

Sr. (a) Encuestado (a)

Se le solicita que responda el presente cuestionario para efectos de la investigación titulada: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMATICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023. Responsable: Bach. Grecia Isabel Herrera Figueroa, para tal efecto se solicita que responda las siguientes preguntas de acuerdo a las alternativas:

5	4	3	2	1
Siempre	Casi siempre	Indiferente	Casi nunca	Nunca

CUESTIONARIO				VALORES				
VARIABLE	DIMENSIONES	INDICADORES	ÍTEMS	5	4	3	2	1
Vx. La incidencia del delito de fraude informático	Actuación de la Policía Nacional del Perú	Detención en flagrancia delictiva	¿La Policía Nacional del Perú detuvo en flagrancia al autor y partícipes del delito?				X	
		Intervenciones a sospechosos	¿La Policía Nacional del Perú intervino a sospechosos del delito?					X
		Recojo de evidencias	¿La Policía Nacional del Perú cuenta con la especialización en el recojo de evidencias del delito de fraude informático?				X	
Vy. Protección efectiva de la víctima	Actuaciones del fiscal de la investigación	Investigaciones fiscales	¿La investigación fiscal fue adecuada?		X			
		Requerimientos de prisión preventiva	¿El fiscal requirió la prisión preventiva del autor y / o partícipes?				X	
		Acusaciones fiscales	¿El fiscal requirió la acusación fiscal?				X	
	Resoluciones del juez penal	Dictó prisión preventiva	¿El juez dictó prisión preventiva al autor y / o partícipes?		X			
		Arribó a terminaciones anticipadas	¿Se arribaron a terminaciones anticipadas con el resarcimiento a la víctima?				X	
		Dictó auto de enjuiciamiento	¿El juez emitió el auto de enjuiciamiento?		X			

Anexo 2. Cuestionario

Sr. (a) Encuestado (a)

Se le solicita que responda el presente cuestionario para efectos de la investigación titulada: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMATICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023. Responsable: Bach. Grecia Isabel Herrera Figueroa, para tal efecto se solicita que responda las siguientes preguntas de acuerdo a las alternativas:

5	4	3	2	1
Siempre	Casi siempre	Indiferente	Casi nunca	Nunca

CUESTIONARIO				VALORES				
VARIABLE	DIMENSIONES	INDICADORES	ÍTEMS	5	4	3	2	1
Vx. La incidencia del delito de fraude informático	Actuación de la Policía Nacional del Perú	Detención en flagrancia delictiva	¿La Policía Nacional del Perú detuvo en flagrancia al autor y partícipes del delito?				X	
		Intervenciones a sospechosos	¿La Policía Nacional del Perú intervino a sospechosos del delito?					X
		Recojo de evidencias	¿La Policía Nacional del Perú cuenta con la especialización en el recojo de evidencias del delito de fraude informático?					X
Vy. Protección efectiva de la víctima	Actuaciones del fiscal de la investigación	Investigaciones fiscales	¿La investigación fiscal fue adecuada?		X			
		Requerimientos de prisión preventiva	¿El fiscal requirió la prisión preventiva del autor y / o partícipes?				X	
		Acusaciones fiscales	¿El fiscal requirió la acusación fiscal?				X	
	Resoluciones del juez penal	Dictó prisión preventiva	¿El juez dictó prisión preventiva al autor y / o partícipes?		X			
		Arribó a terminaciones anticipadas	¿Se arribaron a terminaciones anticipadas con el resarcimiento a la víctima?				X	
		Dictó auto de enjuiciamiento	¿El juez emitió el auto de enjuiciamiento?		X			

Anexo 2. Cuestionario

Sr. (a) Encuestado (a)

Se le solicita que responda el presente cuestionario para efectos de la investigación titulada: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMATICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023. Responsable: Bach. Grecia Isabel Herrera Figueroa, para tal efecto se solicita que responda las siguientes preguntas de acuerdo a las alternativas:

5	4	3	2	1
Siempre	Casi siempre	Indiferente	Casi nunca	Nunca

CUESTIONARIO				VALORES				
VARIABLE	DIMENSIONES	INDICADORES	ÍTEMS	5	4	3	2	1
Vx. La incidencia del delito de fraude informático	Actuación de la Policía Nacional del Perú	Detención en flagrancia delictiva	¿La Policía Nacional del Perú detuvo en flagrancia al autor y partícipes del delito?					X
		Intervenciones a sospechosos	¿La Policía Nacional del Perú intervino a sospechosos del delito?					X
		Recojo de evidencias	¿La Policía Nacional del Perú cuenta con la especialización en el recojo de evidencias del delito de fraude informático?					X
Vy. Protección efectiva de la víctima	Actuaciones del fiscal de la investigación	Investigaciones fiscales	¿La investigación fiscal fue adecuada?					X
		Requerimientos de prisión preventiva	¿El fiscal requirió la prisión preventiva del autor y / o partícipes?		X			
		Acusaciones fiscales	¿El fiscal requirió la acusación fiscal?		X			
	Resoluciones del juez penal	Dictó prisión preventiva	¿El juez dictó prisión preventiva al autor y / o partícipes?				X	
		Arribó a terminaciones anticipadas	¿Se arribaron a terminaciones anticipadas con el resarcimiento a la víctima?		X			
		Dictó auto de enjuiciamiento	¿El juez emitió el auto de enjuiciamiento?				X	

Anexo 2. Cuestionario

Sr. (a) Encuestado (a)

Se le solicita que responda el presente cuestionario para efectos de la investigación titulada: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMATICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023. Responsable: Bach. Grecia Isabel Herrera Figueroa, para tal efecto se solicita que responda las siguientes preguntas de acuerdo a las alternativas:

5	4	3	2	1
Siempre	Casi siempre	Indiferente	Casi nunca	Nunca

CUESTIONARIO				VALORES				
VARIABLE	DIMENSIONES	INDICADORES	ÍTEMS	5	4	3	2	1
Vx. La incidencia del delito de fraude informático	Actuación de la Policía Nacional del Perú	Detención en flagrancia delictiva	¿La Policía Nacional del Perú detuvo en flagrancia al autor y partícipes del delito?					X
		Intervenciones a sospechosos	¿La Policía Nacional del Perú intervino a sospechosos del delito?					X
		Recojo de evidencias	¿La Policía Nacional del Perú cuenta con la especialización en el recojo de evidencias del delito de fraude informático?					X
	Actuaciones del fiscal de la investigación	Investigaciones fiscales	¿La investigación fiscal fue adecuada?					X
Vy. Protección efectiva de la víctima		Requerimientos de prisión preventiva	¿El fiscal requirió la prisión preventiva del autor y / o partícipes?		X			
		Acusaciones fiscales	¿El fiscal requirió la acusación fiscal?		X			
	Resoluciones del juez penal	Dictó prisión preventiva	¿El juez dictó prisión preventiva al autor y / o partícipes?				X	
		Arribó a terminaciones anticipadas	¿Se arribaron a terminaciones anticipadas con el resarcimiento a la víctima?		X			
		Dictó auto de enjuiciamiento	¿El juez emitió el auto de enjuiciamiento?				X	

Anexo 2. Cuestionario

Sr. (a) Encuestado (a)

Se le solicita que responda el presente cuestionario para efectos de la investigación titulada: LA INCIDENCIA DEL DELITO DE FRAUDE INFORMATICO Y LA PROTECCIÓN EFECTIVA DEL CIUDADANO, DISTRITO JUDICIAL DE HUÁNUCO, 2022 – 2023. Responsable: Bach. Grecia Isabel Herrera Figueroa, para tal efecto se solicita que responda las siguientes preguntas de acuerdo a las alternativas:

5	4	3	2	1
Siempre	Casi siempre	Indiferente	Casi nunca	Nunca

CUESTIONARIO				VALORES				
VARIABLE	DIMENSIONES	INDICADORES	ÍTEMS	5	4	3	2	1
Vx. La incidencia del delito de fraude informático	Actuación de la Policía Nacional del Perú	Detención en flagrancia delictiva	¿La Policía Nacional del Perú detuvo en flagrancia al autor y partícipes del delito?			X		
		Intervenciones a sospechosos	¿La Policía Nacional del Perú intervino a sospechosos del delito?		X			
		Recojo de evidencias	¿La Policía Nacional del Perú cuenta con la especialización en el recojo de evidencias del delito de fraude informático?				X	
Vy. Protección efectiva de la víctima	Actuaciones del fiscal de la investigación	Investigaciones fiscales	¿La investigación fiscal fue adecuada?		X			
		Requerimientos de prisión preventiva	¿El fiscal requirió la prisión preventiva del autor y / o partícipes?				X	
		Acusaciones fiscales	¿El fiscal requirió la acusación fiscal?				X	
	Resoluciones del juez penal	Dictó prisión preventiva	¿El juez dictó prisión preventiva al autor y / o partícipes?				X	
		Arribó a terminaciones anticipadas	¿Se arribaron a terminaciones anticipadas con el resarcimiento a la víctima?				X	
		Dictó auto de enjuiciamiento	¿El juez emitió el auto de enjuiciamiento?				X	