Universidad Nacional Federico Villarreal

VRIN | VICERRECTORADO DE INVESTIGACIÓN

FACULTAD DE DERECHO Y CIENCIA POLÍTICA

EFICACIA DE LA INVESTIGACIÓN FISCAL DE LOS DELITOS INFORMÁTICOS EN LAS FISCALÍAS ESPECIALIZADAS EN CIBERDELINCUENCIA DE LIMA CENTRO, 2024

Línea de investigación:
Procesos jurídicos y resolución de conflictos

Tesis para optar el Título Profesional de Abogado

Autora

Falcon Vilela, Paola Alexandra

Asesor

Jiménez Herrera, Juan Carlos

ORCID: 0000-0001-9996-2047

Jurado

Gonzales Loli, Martha Rocio

Moscoso Torres, Víctor Juber

Mendoza La Rosa, Carlos Alfonso

Lima - Perú

2026

TESIS PAOLA FALCON.docx

INFORME DE ORIGINALIDAD

24%	22%	7%	11%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	hdl.handle.net Fuente de Internet	5%
2	Submitted to Universidad Nacional Federico Villarreal Trabajo del estudiante	1%
3	Submitted to UNIBA Trabajo del estudiante	1%
4	repositorio.ucv.edu.pe Fuente de Internet	1%
5	revistas.pj.gob.pe Fuente de Internet	1%
6	repositorio.upsjb.edu.pe Fuente de Internet	1%
7	repositorio.autonoma.edu.pe Fuente de Internet	1%
8	es.scribd.com Fuente de Internet	1%
9	repositorio.unfv.edu.pe Fuente de Internet	1%
10	www.coursehero.com Fuente de Internet	1%
11	Submitted to usmp Trabajo del estudiante	<1%
12	www.defensoria.gob.pe Fuente de Internet	<1%

FACULTAD DE DERECHO Y CIENCIA POLÍTICA

EFICACIA DE LA INVESTIGACIÓN FISCAL DE LOS DELITOS INFORMÁTICOS EN LAS FISCALÍAS ESPECIALIZADAS EN CIBERDELINCUENCIA DE LIMA CENTRO, 2024.

Línea de investigación

Procesos Jurídico y Resolución de conflictos

Tesis para optar el Título Profesional de Abogado

Autora

Falcon Vilela, Paola Alexandra

Asesor

Jiménez Herrera, Juan Carlos

ORCID: 0000-0001-9996-2047

Jurado:

Gonzales Loli, Martha Rocio

Moscoso Torres, Víctor Juber

Mendoza La Rosa, Carlos Alfonso

Lima – Perú

2026

DEDICATORIA

A mi madre, por enseñarme el significado de la perseverancia; por su bondad y amor infinito. Por fortalecer mi integridad y dignidad como mujer, y su apoyo incondicional hacia mi persona.

A mi padre por enseñarme el significado del esfuerzo, humildad, trabajo y disciplina. A mi hermano; por enseñarme el significado de la hermandad; por su determinación, apoyo y gratitud hacia mi persona. A mis dos ángeles en el cielo, mi abuelita Consuelo y mi primo Jorge, por enseñarme el significado de la resiliencia, amor hacia el prójimo; por la confianza, cuidado y respeto hacia mi persona.

AGRADECIMIENTOS

A mi asesor, Dr. Juan Carlos Jiménez Herrera, por su tiempo y profesionalismo para la realización de este proyecto.

Abog. Hellen Mautino, por su paciencia y colaboración para la elaboración de este proyecto.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Objetivo: Identificar las causas que limitan realizar una persecución eficaz al delito informático, en las fiscalías de Ciberdelincuencia de Lima Centro, 2023. **Método:** El estudio se realizó mediante el enfoque cualitativo, de tipo básico, los instrumentos de recolección de datos de observación, entrevista y análisis documental. **Resultados:** Los resultados evidenciaron que el delito informático representó una amenaza creciente que compromete diversos bienes jurídicos; pues, los especialistas coinciden en que factores como el desconocimiento de las víctimas, la deficiente seguridad institucional y la limitada colaboración de entidades privadas obstaculizan su persecución; paralelamente, resaltaron la necesidad de medidas correctivas como la capacitación especializada, el acceso oportuno a información y la implementación de mecanismos tecnológicos. **Conclusiones:** Las conclusiones revelaron que la persecución del delito informático es limitada por factores como el desconocimiento de las víctimas, la brecha digital, la débil ciberseguridad institucional y la omisión de las entidades financieras; además, la falta de identificación de los responsables conllevar impunidad y archivamiento de denuncias; por ello, se arribó a la conclusión de que es necesario implementar medidas correctivas centradas en la articulación interinstitucional, capacitación especializada, acceso eficiente a la información y sanciones efectivas a entidades que incumplen sus funciones preventivas.

Palabras claves: Persecución eficaz, delito informático, ciberdelincuencia.

ABSTRACT

Objective: To identify the factors that hinder the effective prosecution of cybercrime in the Cybercrime Prosecutor's Offices of Central Lima, 2023. **Method:** The study employed a qualitative, basic-type approach, using observation, interviews, and document analysis as data collection instruments. **Results:** The findings revealed that cybercrime constitutes a growing threat affecting various legal interests. Experts agreed that factors such as victims' lack of awareness, weak institutional security, and limited cooperation from private entities obstruct effective prosecution. Simultaneously, they emphasized the need for corrective measures such as specialized training, timely access to information, and the implementation of technological mechanisms. **Conclusions:** The study concluded that the prosecution of cybercrime is hindered by factors including victims' lack of knowledge, the digital divide, weak institutional cybersecurity, and negligence by financial institutions. Furthermore, the inability to identify perpetrators results in impunity and case dismissals. Therefore, it is necessary to implement corrective measures focused on inter-institutional coordination, specialized training, efficient access to information, and effective sanctions against entities that fail to fulfill their preventive responsibilities.

Keywords: Effective prosecution, cybercrime, cyber delinquency.

I. INTRODUCCIÓN

El desarrollo exorbitante del uso de las tecnologías de la información ha cambiado de manera relevante la forma en que las personas interactúan y acceden a servicios, generando nuevas oportunidades, pero también nuevos riesgos; en este contexto la era digital ha desafiado los parámetros legales como lo son los delitos informáticos; los cuales han emergido como una amenaza compleja y en constante evolución, que desafía a los sistemas tradicionales de justicia penal, tanto en su detección como en su persecución.

En el Perú, y particularmente en Lima Centro, esta problemática se manifiesta en el incremento sostenido de denuncias vinculadas a ciberdelitos y en las dificultades estructurales y operativas que enfrentan las Fiscalías Especializadas en Ciberdelincuencia para abordarlos de manera oportuna y eficaz.

El problema principal que se examina en este estudio es la poca efectividad en la acción penal contra los delitos cibernéticos en las Fiscalías de Ciberdelincuencia de Lima Centro. Esto sucede por razones como la falta de leyes adecuadas, la escasez de tecnología, la limitada formación especializada del personal fiscal y la ausencia de cooperación entre las entidades que investigan los delitos digitales. Esta ineficiencia afecta la protección de los derechos fundamentales de las víctimas, el respeto al debido proceso y la capacidad del sistema de justicia penal para responder a las nuevas formas de criminalidad en línea.

La presente investigación se desarrolla en ocho capítulos, organizados de manera que permiten un abordaje progresivo, riguroso y articulado del objeto de estudio. El primer capítulo comprende la descripción detallada de la situación problemática, en la que se expone el contexto general y específico de la ciberdelincuencia en Lima Centro, identificando el problema general y los problemas específicos que motivan el estudio.

El segundo capítulo desarrolla el marco teórico, donde se sistematizan las principales categorías conceptuales, enfoques doctrinarios y disposiciones normativas relacionadas con el sistema acusatorio penal, los delitos informáticos, la función de las Fiscalías Especializadas en Ciberdelincuencia y el fenómeno de la ciberdelincuencia en general.

El tercer capítulo está dedicado al método de investigación, en el que se describe el tipo de estudio adoptado, el ámbito referente al tiempo y espacio en el que se desarrolla, la categorización de variables, las unidades de análisis seleccionadas, las formas de recopilación de datos y los procesos utilizados, además de las consideraciones éticas relevantes.

El cuarto capítulo presenta los resultados del trabajo de campo, obtenidos a partir de técnicas cualitativas, las cuales permiten evidenciar las principales falencias en la persecución de los delitos informáticos y las condiciones institucionales de las fiscalías evaluadas.

El quinto capítulo, se centra en los resultados adquiridos a lo largo de esta investigación, los cuales permitieron corroborar los objetivos planteados y responder a la hipótesis de trabajo. De esa forma, a través del análisis documental, la aplicación de encuestas y entrevistas (según la metodología utilizada), se identificaron los aspectos clave del problema investigado y se evidenció la necesidad de implementar mejoras en las prácticas observadas.

El sexto capítulo, refiere a las conclusiones las cuales hemos logrado concretar en referencia al contexto de la investigación. De esa forma, se llegó a la conclusión de que la problemática abordada se encuentra arraigada en múltiples niveles, siendo el desfase entre la norma y su aplicación uno de los factores más determinantes.

El séptimo capítulo, alude a las recomendaciones En función de los resultados y conclusiones obtenidas, se formula un conjunto de recomendaciones orientadas a contribuir con la mejora del abordaje del problema tratado. Siendo así que, desarrollar las

recomendaciones correctas es necesario, de tal modo que se garantice una implementación adecuada y coherente con los principios del sistema normativo vigente.

En conjunto, esta estructura busca aportar elementos teóricos, empíricos y propositivos que permitan fortalecer el sistema de justicia penal frente a los delitos informáticos y garantizar una persecución eficaz en el marco del Estado constitucional de derecho.

1.1. Descripción de la situación problemática

En el contexto internacional, el delito informático se ha convertido en una de las amenazas más complejas y dinámicas del siglo XXI, pues afecta a la seguridad jurídica de los Estados y desafiando la eficacia de los sistemas de persecución penal; ya que, la globalización digital permitió la expansión transfronteriza de conductas ilícitas como el fraude electrónico, la suplantación de identidad y el acceso indebido a sistemas informáticos, dificultando su tipificación, rastreo y sanción.

Es entonces que, la carencia de mecanismos armonizados entre jurisdicciones, así como la limitada cooperación interestatal, han contribuido a que estas conductas se perpetúen con altos niveles de impunidad; aunado a ello, se suma que la legislación internacional actual no ha sido actualizada para responder a la sofisticación técnica del cibercrimen, lo que obstaculiza su tratamiento eficaz por parte de los entes fiscales

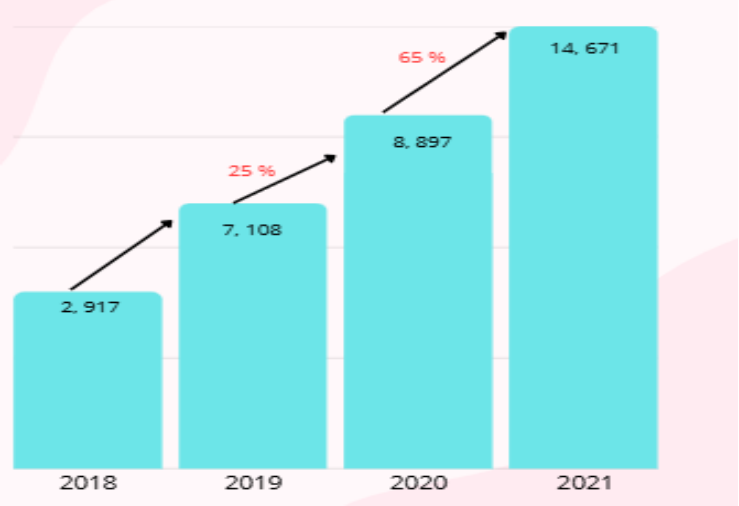
En el Perú, si bien se ha avanzado en la incorporación de tipos penales vinculados al delito informático mediante la Ley N.º 30096, aún subsisten vacíos normativos, deficiencias técnicas y limitaciones logísticas que afectan su adecuada persecución; puesto que, las fiscalías especializadas en ciberdelincuencia se enfrentan a un entorno hostil, caracterizado por la falta de recursos tecnológicos, capacitación insuficiente del personal fiscal y una carga procesal elevada; además, la celeridad con la que evolucionan las tecnologías supera la capacidad de reacción del sistema penal, generando una brecha entre el delito y su sanción. En consecuencia, la respuesta del Estado resulta ineficaz para garantizar la protección de los derechos fundamentales vulnerados por estas conductas (Carrillo y Montenegro, 2018).

En los últimos años se han incrementado las modalidades delictivas a través de los medios informáticos en nuestro país, a tal punto que por política criminal el Estado ha dictado la LEY Nº 30096 con el objeto de combatir eficazmente la lucha contra las diferentes

modalidades delictivas del delito informático. Así le da cuenta el Ministerio de Justicia una de sus recientes publicaciones:

Figura 1

Crecimiento de delito informático



Fuente: Ministerio de Justicia.

Se advierte del presente gráfico que en los últimos cuatro años se registraron 2 mil 917 denuncias en el año 2018, hasta llegar a 14 mil 671 denuncias en el año 2021. Además, es posible observar que entre 2018 y 2021 las denuncias se han incrementado de manera constante.

En Lima, específicamente en el ámbito de las Fiscalías de Ciberdelincuencia de Lima Centro, esta problemática se agudiza debido al incremento sostenido de denuncias por delitos informáticos, sin que exista una estrategia integral para su tratamiento; puesto que, a pesar de contar con una jurisdicción focalizada, la sobrecarga de casos, la escasa articulación con otras entidades del sistema judicial y la limitada interoperabilidad tecnológica con las fuerzas policiales comprometen la eficacia del proceso penal; así mismo, la conducta pasiva o poco diligente de algunos sujetos procesales, como fiscales o peritos, obstaculiza el esclarecimiento de los hechos y la obtención de pruebas digitales válidas (Jiménez, 2023).

Entre las causas principales que impiden una persecución eficaz del delito informático se encuentran la inadecuada capacitación de los operadores jurídicos, la escasa sensibilización respecto a la relevancia probatoria de la evidencia digital, y la insuficiencia de infraestructura tecnológica en el Ministerio Público; en consecuencia, estas falencias estructurales son agravadas por una cultura institucional que prioriza la carga resolutiva antes que la calidad de la actuación fiscal; además, la conducta de ciertos sujetos procesales como la pasividad del fiscal frente a requerimientos técnicos o la descoordinación con la Policía Nacional refleja una desconexión entre el diseño normativo y la práctica procesal cotidiana (Ponds, 2017).

Las consecuencias derivadas de esta problemática se manifiestan en altos niveles de impunidad, pérdida de confianza ciudadana en el sistema de justicia penal, y una creciente victimización de usuarios digitales; pues tenemos que, la ineficacia en la persecución del delito informático no solo obstaculiza la tutela efectiva de los derechos vulnerados, sino que también fomenta la reincidencia delictiva y el crecimiento de redes delictivas organizadas en entornos digitales.

Frente a este panorama, resulta imperativo proponer una estrategia integral que permita optimizar la labor de las fiscalías especializadas; la cual, deba contemplar la capacitación constante en criminalística digital, el fortalecimiento de la cooperación interinstitucional y el uso de herramientas tecnológicas adecuadas para la investigación del delito informático.

1.1.1. Problema General.

¿Cómo influye la investigación fiscal en la eficacia de la sanción de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024?

1.1.2. Problemas Específicos.

El trabajo de investigación propone los siguientes problemas secundarios a través de las siguientes preguntas:

P.1. ¿Cuáles son las causas que limitan realizar una persecución eficaz de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024?

P.2. ¿Cuáles son las consecuencias que conlleva la falta de identificación de los partícipes del delito informático para garantizar una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024?

P.3. ¿Cuáles serían las medidas correctivas que deberían adoptarse para realizar una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024?

1.2. Antecedentes

1.2.1 Antecedentes Internacionales

Barrionuevo (2016) investigó los delitos informáticos que afectan a las entidades financieras cooperativas del segmento uno de la economía popular y solidaria en el Cantón Ambato, Provincia de Tungurahua. Su tesis de pregrado de la Universidad Técnica de Ambato tuvo como objetivo examinar estos delitos dentro de la fiscalía. Para ello, se desarrolló un Manual General de Procedimiento para casos de delitos informáticos, abarcando fases de análisis, diseño, desarrollo, implantación, implementación y evaluación. Las conclusiones destacaron que los delitos más comunes en estas instituciones incluyen fraudes por manipulación informática, sabotajes, ataques de virus y accesos no autorizados a sistemas, actos que, según Barrionuevo, comprometen gravemente el derecho a la seguridad de la información de socios y clientes.

Toledo y Venegas (2020), en su tesis para optar al grado de Licenciado en Ciencias Jurídicas y Sociales en la Universidad de Chile, analizaron las herramientas previstas en el Convenio de Budapest sobre Ciberdelincuencia y su adecuación a la legislación chilena.

El estudio tuvo como objetivo principal examinar, a partir de fuentes nacionales e internacionales, la implementación de este acuerdo global y su impacto en la investigación de delitos informáticos, así como su eventual incorporación en las normativas internas, procurando siempre garantizar la proporcionalidad y el respeto de los derechos fundamentales. La investigación, de enfoque cualitativo, concluyó que, si bien el convenio fue ambicioso en sus inicios, diecinueve años después de su adopción resulta insuficiente para abarcar todos los desafíos que plantea la ciberdelincuencia en la actualidad. Un ejemplo de esto es la falta de regulación para figuras de investigación como el agente encubierto en línea. Esto significa que, si bien el convenio es un buen punto de partida, los países tienen la responsabilidad de complementar sus leyes para mantenerse al día con el rápido avance de la tecnología.

La tesis de maestría de Torres (2019) de la Universidad Santander (UDES) tuvo como objetivo principal determinar si la tipificación actual de los delitos informáticos está alineada con el avance digital y tecnológico entre 2009 y 2018. Para lograrlo, Torres utilizó una metodología jurídico-sistémica-cualitativa que combinó un método teórico-analítico y propositivo. Basándose en esto, se propuso un nuevo conjunto de reglas legales para la modernización de las normativas en Colombia. Estas se presentaron en un "Modelo completo de salvaguarda de datos e información en el ámbito tecnológico y digital: Estudio de acciones no definidas en la legislación penal entre 2009 y 2018". La investigación concluyó que la globalización y los avances en las comunicaciones han creado un escenario virtual donde las barreras físicas ya no son un impedimento en el ámbito jurídico-penal para la comisión de delitos informáticos, ya que la presencia física del perpetrador ya no es necesaria.

López (2023), Indagación de la ciberdelincuencia por parte de la policía y habilidad para reaccionar a través del Proyecto Cyberwall, en cuanto a formación y capacitación de la Policía Nacional. Tesis de doctorado, Universidad salmantina.

Esta investigación analiza la relevancia de la formación como elemento clave para que la Policía Nacional pueda adaptarse a los retos que plantea la ciberseguridad y la ciberdelincuencia. Contempla una revisión exhaustiva de literatura especializada, así como el análisis de casos de estudio y experiencias prácticas sobre formación en ciberseguridad policial. Asimismo, examina los programas de capacitación vigentes, tanto en el Perú como en otros países, con el fin de identificar buenas prácticas y formular recomendaciones que fortalezcan la capacidad de respuesta policial frente al cibercrimen. Los resultados buscan ofrecer una comprensión más amplia de los desafíos y oportunidades que la ciberseguridad representa para las fuerzas del orden, resaltando la necesidad de una capacitación continua y de la actualización permanente de conocimientos en un ámbito en constante cambio.

1.1.2 Antecedentes Nacionales

Peralta (2022). Los delitos cibernéticos y la información en sistemas de computación. Tesis de grado, Universidad Peruana de las Américas.

El presente trabajo tiene como objetivo analizar el incremento de las amenazas a los sistemas informáticos como consecuencia de los delitos cibernéticos en un contexto de creciente globalización y digitalización. Se busca evidenciar el impacto de estas conductas en los derechos fundamentales de las personas y en la seguridad jurídica en el Perú. Este fenómeno se desarrolla en un escenario donde el uso de las tecnologías de la información y la comunicación se ha convertido en un elemento indispensable para el desarrollo y la modernización, tanto en el ámbito público como en el privado. La investigación adopta un enfoque cualitativo y un análisis descriptivo de la problemática actual, centrado en la

penetración de los sistemas informáticos por parte de ciberdelincuentes. Se observa que, mediante diversas modalidades de intrusión, estos logran acceder y sustraer información sensible desde cualquier parte del mundo, afectando a instituciones públicas, entidades financieras y empresas privadas. Se concluye que la magnitud de esta amenaza demanda una respuesta eficaz y actualizada por parte de los operadores de justicia. Es fundamental que las autoridades encargadas de la investigación y persecución penal estén debidamente capacitadas y tecnológicamente preparadas para enfrentar los desafíos que implica la recolección de pruebas digitales.

Milla (2021) El delito informático y lo que le falta a su legislación. En la tesis de licenciatura de Usan (Universidad San Andrés). La presente tesis tuvo como objetivo general analizar la vulnerabilidad de los sistemas informáticos frente a los delitos cibernéticos en un contexto globalizado, así como los efectos que estos generan sobre los derechos fundamentales de las personas y la seguridad jurídica del Estado. Con ello, se busca evidenciar la necesidad de fortalecer la capacidad de respuesta de los operadores de justicia en la recolección de pruebas digitales y en la persecución penal efectiva de los ciberdelitos. La investigación se desarrolla bajo un enfoque cualitativo de tipo descriptivo, sustentado en el análisis documental y conceptual sobre la incidencia de los delitos informáticos en el Perú y en el ámbito internacional. Se examina la forma en que los ciberdelincuentes vulneran los sistemas informáticos de instituciones públicas, entidades bancarias y empresas privadas para sustraer información y obtener beneficios económicos ilícitos. Asimismo, se evalúa el nivel de preparación de los operadores de justicia ante estos desafíos, en un contexto marcado por el uso creciente de las tecnologías de la información y la comunicación (TIC) tanto en el funcionamiento del Estado como en la vida cotidiana.

La investigación concluye que los delitos informáticos constituyen una amenaza transnacional que pone en riesgo la integridad de los datos personales, la seguridad financiera

y la estabilidad jurídica de los Estados. En el caso peruano, si bien el uso de las TIC se ha incorporado a las políticas públicas de modernización, la respuesta frente a la ciberdelincuencia aún presenta deficiencias. Resulta imprescindible que los operadores de justicia actualicen sus capacidades técnicas y jurídicas para afrontar estos delitos con eficacia, especialmente en la recolección, tratamiento y valoración de las pruebas digitales, con el fin de prevenir la impunidad y garantizar una protección efectiva de los derechos fundamentales en el entorno digital.

Matos (2022). Especialización de la investigación preliminar en delitos informáticos relacionados con fraudes. En el trabajo de grado de la Universidad César Vallejo.

Este estudio tuvo como propósito analizar la aplicación de la investigación preparatoria en los casos de fraude informático tramitados en el Ministerio Público de Lima Norte. Se adoptó un enfoque cualitativo, de tipo aplicado y con un diseño basado en la teoría fundamentada. La recolección de información se realizó mediante entrevistas y análisis documental, lo que permitió obtener datos pertinentes, confiables y actualizados, garantizando que los resultados reflejaran con precisión la realidad estudiada.

Los hallazgos evidencian la necesidad de modificar la legislación sobre delitos cibernéticos y de modernizar las herramientas tecnológicas vinculadas a su investigación. Asimismo, se requiere optimizar el sector logístico, fortalecer la capacitación de los operadores jurídicos encargados de estos casos y reforzar la estructura del Ministerio Público y de la DIVINDAT de la Policía Nacional del Perú. En este marco, se plantea una propuesta dirigida a que las autoridades competentes consideren e implementen estas recomendaciones.

(2024) Orellano y Galindo. Faltas en la legislación relacionadas con la Ley N° 30096, Ley de delitos informáticos – fraude informático, Lima, durante el periodo de 2019 a 2021. El objetivo de esta investigación fue detectar las fallas en la legislación con respecto a la

implementación de la Ley N° 30096 (Ley de Delitos Informáticos - Fraude Informático) en Lima, durante el lapso de tiempo comprendido entre 2019 y 2021. Aunque el marco teórico considera tanto enfoques cualitativos como cuantitativos, esta investigación se centró principalmente en un análisis cualitativo. Esto se debe a que no se trabajaron con datos numéricos, sino que se examinaron los hechos conforme se presentaban, siendo esta la metodología más adecuada para el objetivo planteado.

La investigación concluyó que el fraude informático se define como una acción ilegal realizada por alguien con conocimientos informáticos o que utiliza las Tecnologías de la Información y Comunicación (TIC). Este delito se lleva a cabo usando herramientas informáticas a través de internet y/o mediante la obtención de datos personales. Su fin es vulnerar la intimidad y privacidad de las víctimas, causando un perjuicio económico a personas o empresas al acceder ilegalmente a cuentas bancarias, billeteras digitales o similares.

La calificación fiscal de los delitos cibernéticos en el distrito fiscal de Lima Centro, 2019-2020, según Sotomayor (2022). En la tesis de maestría que se realizó en la Universidad César Vallejo.

Este estudio se centró en cómo la calificación fiscal impacta la investigación de delitos informáticos en el Distrito Fiscal de Lima Centro durante 2019-2020. La investigación utilizó un enfoque cualitativo, con un diseño basado en la teoría fundamentada.

La principal conclusión fue que, durante el período analizado, la calificación fiscal de los delitos informáticos no fue siempre la adecuada para determinar la existencia de estos crímenes. A menudo, la naturaleza del delito cambiaba durante la investigación, derivando en una calificación diferente al final. Por ejemplo, aunque inicialmente se investigaba como delito informático, la formalización terminaba siendo por hurto agravado.

1.3. Objetivos

1.3.1. Objetivo general.

Determinar cómo influye la investigación fiscal en la eficacia de la sanción de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

1.3.2. Objetivos Específicos

O.1. Determinar cuáles son las causas que limitan realizar una persecución eficaz de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

O.2. Determinar cuáles son las consecuencias que conlleva la falta de identificación de los partícipes del delito informático para garantizar una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

O.3. Determinar cuáles serían las medidas correctivas que deberían adoptarse para realizar una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

1.4. Justificación

Esta tesis se plantea justificar sosteniendo los siguientes tipos de justificación:

1). Justificación Teórica

La presente investigación se ha basado en examinar la figura jurídica del delito informático, para estudiar su naturaleza jurídica.

2). Justificación Práctica

La presente investigación tiene como sustento la práctica, ya que, tiene la necesidad de garantizar el derecho a la propiedad y el honor de las personas que utilizan los medios informáticos, así como de hacer una eficaz lucha contra esa modalidad delictiva.

3). Justificación Metodológica

La actual investigación se sustenta metodológicamente en vista que utiliza el enfoque cualitativo de investigación aplicando como instrumento y técnica de estudio las guías de entrevistas y analiza documentalmente la doctrina, jurisprudencia y la ley; así como además proponer lineamientos correctivos a adoptarse por parte del Estado.

1.5. Hipótesis

1.5.1. Hipótesis general

La investigación fiscal influye en la eficacia de la sanción de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

1.5.2. Hipótesis específicas

H.1. La falta de capacitación fiscal, actualización digital de los despachos, falta de actividad probatoria que permita identificar el sujeto del delito se relacionan como causas que afectan la investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

H.2. La ineficacia de la investigación fiscal de los delitos informáticos ocasiona la falta de identificación de los partícipes del delito; en consecuencia, se archivan definitivamente las denuncias penales en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

H.3. La implementación de medidas correctivas permitiría una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

II. MARCO TEÓRICO

2.1. Bases teóricas sobre el tema de investigación

2.1.1. Delitos informáticos

Clavijo (2015) define a los delitos informáticos son aquellas acciones antijurídicas, culpables y típicas que se realizan mediante el uso de computadoras, redes o sistemas informáticos, o bien que tienen como objetivo dañar, acceder, modificar, destruir o robar información o sistemas de datos sin autorización. (p.34).

Silva (2012) se entiende por delitos informáticos aquellas conductas que lesionan bienes jurídicos protegidos por el Derecho Penal a través del uso indebido de sistemas informáticos o de la manipulación de datos almacenados en soportes electrónicos. (p. 118).

Ayma (2020), define como delito informático a cualquier actividad ilícita realizada mediante el uso indebido de sistemas informáticos contra personas naturales o jurídicas, en violación de las normas vigentes, y que, por lo tanto, puede ser sancionada por el derecho penal. (p. 40).

Mendoza (2017) el delito informático no solo se limita al fraude computacional o al acceso ilícito, sino que abarca una gama amplia de comportamientos que van desde el ciberacoso hasta la pornografía infantil, siempre con un factor común: el uso de la informática como medio o fin del delito. (p. 67).

Sánchez (2018) los delitos informáticos son aquellos actos ilegales que se realizan utilizando medios cibernéticos o informáticos o redes de comunicación; y que pueden afectar la seguridad, la privacidad y los derechos de los usuarios.

El delito informático se define como una conducta típica y antijurídica en la que el autor utiliza el ciberespacio y los sistemas informáticos como medios para ejecutar actos ilícitos.

Estas conductas afectan o ponen en riesgo bienes jurídicos —tanto convencionales como emergentes— que cuentan con protección legal.

En sus inicios, los delitos cibernéticos fueron abordados por los Estados a través de marcos normativos tradicionales, aplicando disposiciones sobre robo, fraude, falsificación, estafa o sabotaje. Sin embargo, el uso indebido de las tecnologías de la información evidenció la necesidad de una regulación específica, dado que el avance tecnológico ha facilitado la aparición de nuevas modalidades delictivas difíciles de encajar en las figuras jurídicas clásicas. Esta situación ha generado un debate jurídico en torno a la importancia de diferenciar con precisión las infracciones tradicionales de los delitos informáticos y de establecer definiciones claras en la legislación.

En ese sentido, los delitos informáticos pueden entenderse como conductas criminales que emplean las tecnologías informáticas como método, medio o fin en entornos virtuales. Desde una perspectiva más específica, se definen como todo acto ilícito penal en que las plataformas digitales, sus técnicas, funciones, desempeñan un papel esencial en la comisión del hecho.

Dentro de esta categoría, se distinguen dos modalidades principales:

- **Delitos informáticos típicos**: conductas antijurídicas y culpables en las que la computadora o el sistema informático se utiliza como instrumento directo para la ejecución del delito.
- **Delitos informáticos atípicos**: aquellos en los que el uso de las tecnologías de la información no encaja plenamente en las figuras penales previstas, pero que igualmente generan un impacto jurídico y social significativo.

A pesar de que los conceptos universales sobre delitos informáticos siguen vigentes, los avances normativos impulsados por las autoridades han permitido desarrollar definiciones más prácticas y modernas. Estos esfuerzos han identificado problemáticas nacionales específicas y han tipificado de manera más detallada determinadas conductas delictivas en el entorno digital. Sin embargo, los delitos informáticos continúan evolucionando con mayor sofisticación, favorecidos por la creciente vulnerabilidad de los sistemas y de los propios usuarios.

En este contexto, la seguridad en internet se ha convertido en un elemento crítico, lo que genera graves impactos en la vida cotidiana, con miles de agresiones diarias perpetradas por actores estatales, organizaciones y ciberdelincuentes. Para que un hecho sea considerado delito, debe tener relevancia jurídica y estar previsto en el Código Penal, conforme al principio de legalidad. Esto significa que únicamente pueden sancionarse aquellas acciones que estén expresamente tipificadas en la normativa penal, quedando excluidas las conductas que no se encuadren en un tipo penal definido.

Por su parte, el ciber-delito, o delito informático, se define como aquel en el que las tecnologías de la información y la comunicación se emplean como herramientas para la comisión de conductas ilícitas, con el propósito de acceder, manipular o apropiarse de sistemas de almacenamiento de información.

Este tipo de criminalidad implica acciones orientadas a eludir los sistemas de seguridad, invadiendo archivos alojados en computadoras y obteniendo las claves necesarias para su acceso. Con frecuencia, este proceso se lleva a cabo mediante el uso de software sofisticado, capaz de vulnerar incluso los sistemas de protección más robustos (Ayma, 2020).

En relación, se sostiene que el delito informático consiste en el uso de cualquier sistema informático como instrumento para la comisión de una conducta ilícita.

Los crímenes cibernéticos comprenden acciones ilegales que, mediante el empleo de tecnología informática, alteran o afectan la memoria de computadoras, redes de internet o dispositivos electrónicos.

Estas actividades ilícitas han sido enfrentadas por los Estados sin una plena comprensión de su alcance y complejidad. A diferencia de los delitos tradicionales, que suelen dejar evidencias físicas y pueden ser probados mediante medios materiales, los delitos informáticos se ejecutan en tiempo real, trascienden fronteras sin requerir la presencia física del autor y se valen de herramientas tecnológicas que dificultan su detección y persecución.

El delito cibernético abarca una variedad de actos ilícitos que las autoridades de distintos países han intentado priorizar. Sin embargo, el problema está en que estos delitos no están debidamente tipificados en el área penal. En lugar de clasificar estos delitos con base en figuras tradicionales como robo, fraude o estafa, es necesario que las autoridades modernicen sus normativas para abordar eficazmente estos crímenes utilizando herramientas tecnológicas.

2.1.1.1. Antecedentes históricos de los delitos informáticos

Los antecedentes de los delitos informáticos surgen paralelamente al desarrollo del internet y el desarrollo global de la informática.

Desde los años sesenta, la preocupación por el almacenamiento y procesamiento de datos personales en ordenadores digitales empezó a aparecer en la literatura y en la opinión pública.

En la década de los años 1970, se empezaron a registrar las primeras manifestaciones de delincuencia informática, especialmente en el ámbito empresarial y bancario. Los delitos más comunes eran el fraude, el sabotaje, la manipulación de datos y el espionaje informático. En 1973, un cajero de Nueva York utilizó una computadora para desviar más de dos millones de dólares, uno de los primeros casos documentados de fraude informático.

El uso masivo de Internet en los años 90 marcó un punto de inflexión, ya que permitió que los delitos se expandieran a escala internacional. Es así como surgen nuevos delitos como el phishing, el hackeo, la distribución de virus, la pornografía infantil en línea, entre otros. En 1997, la OCDE emite directrices sobre seguridad de los sistemas de información.

En el año 2001, se firma el Convenio de Budapest sobre Ciberdelincuencia, promovido por el Consejo de Europa, el cual es el primer tratado internacional que aborda los delitos informáticos de forma integral.

2.1.1.2. Base normativo de los delitos informáticos

A continuación, se realizará una descripción de la base normativa en nuestra legislación nacional sobre los delitos informáticos:

- **Ley N.° 30096, Ley de Delitos Informáticos:** Esta normativa sienta la base principal para prevenir y castigar acciones ilegales que afectan los sistemas y datos informáticos en Perú. Asimismo, el propósito de esta ley es asegurar una lucha efectiva contra el crimen cibernético, protegiendo tanto la información como los sistemas tecnológicos de individuos y organizaciones.
- **Reglamento de la Ley de delitos informáticos, Decreto Supremo N.° 030-2019-JUS:** Desarrolla los procedimientos para aplicar la Ley 30096 y establece Facultades de la Policía Nacional en investigaciones digitales.

2.1.1.3. Las categorías de los delitos informáticos

Según Frank Almanza (2024), en el Perú, los delitos cibernéticos son acciones ilegales que se realizan usando computadoras o redes de internet. Pueden poner en riesgo la seguridad, la privacidad y los derechos de las personas que usan estas plataformas. Incluyen, el robo de datos personales o financieros, así como el daño o alteración de sistemas informáticos.

Los delitos cibernéticos son un problema que cambia y crece con rapidez, porque los delincuentes usan herramientas cada vez más avanzadas para cometerlos. No solo afectan a personas y empresas, sino también a los gobiernos y a la seguridad del país. Los hackers pueden atacar sistemas importantes, lo que podría causar graves daños a la economía y a la seguridad nacional.

También es importante entender que los delitos informáticos no son exclusivos de los expertos en informática, sino que cualquier persona con acceso a una computadora e internet puede cometer un delito cibernético.

De acuerdo con el libro de Frank Almazan, señala las cinco categorías fundamentales de los delitos cibernéticos, siendo: **acceso no autorizado**, **robo de información**, **fraude en línea**, **malware** y **ciberacoso**.

En primer lugar, el **acceso no autorizado** ocurre cuando alguien entra a un sistema informático sin permiso. Esto puede hacerse robando contraseñas, probando muchas combinaciones hasta encontrar la correcta o aprovechando fallas del sistema. Estas acciones ponen en riesgo la confidencialidad y la seguridad de la información.

En segundo lugar, el r**obo de información** ocurre cuando se obtienen datos de forma ilegal, afectando la privacidad y los bienes de las personas. Los datos más vulnerables son los personales, financieros y comerciales, que pueden usarse para fraudes, suplantaciones o venderse en el mercado ilegal.

Y como tercera categoría alude al **fraude en línea**, por su parte, engloba los engaños cometidos en entornos virtuales con el objetivo de obtener algún beneficio económico o personal. Las principales formas de fraude señaladas en el gráfico son el uso de sitios web falsos y el engaño directo a usuarios, mediante técnicas como el phishing o suplantación de identidad digital.

Otro tipo importante de delito informático es el **uso de malware**, que consiste en programas maliciosos diseñados para dañar, infiltrar o controlar sistemas informáticos. Dentro de esta categoría se encuentran los virus, troyanos, ransomware (que bloquea archivos y exige un pago para liberarlos) y otros programas similares que afectan la integridad y disponibilidad de los sistemas.

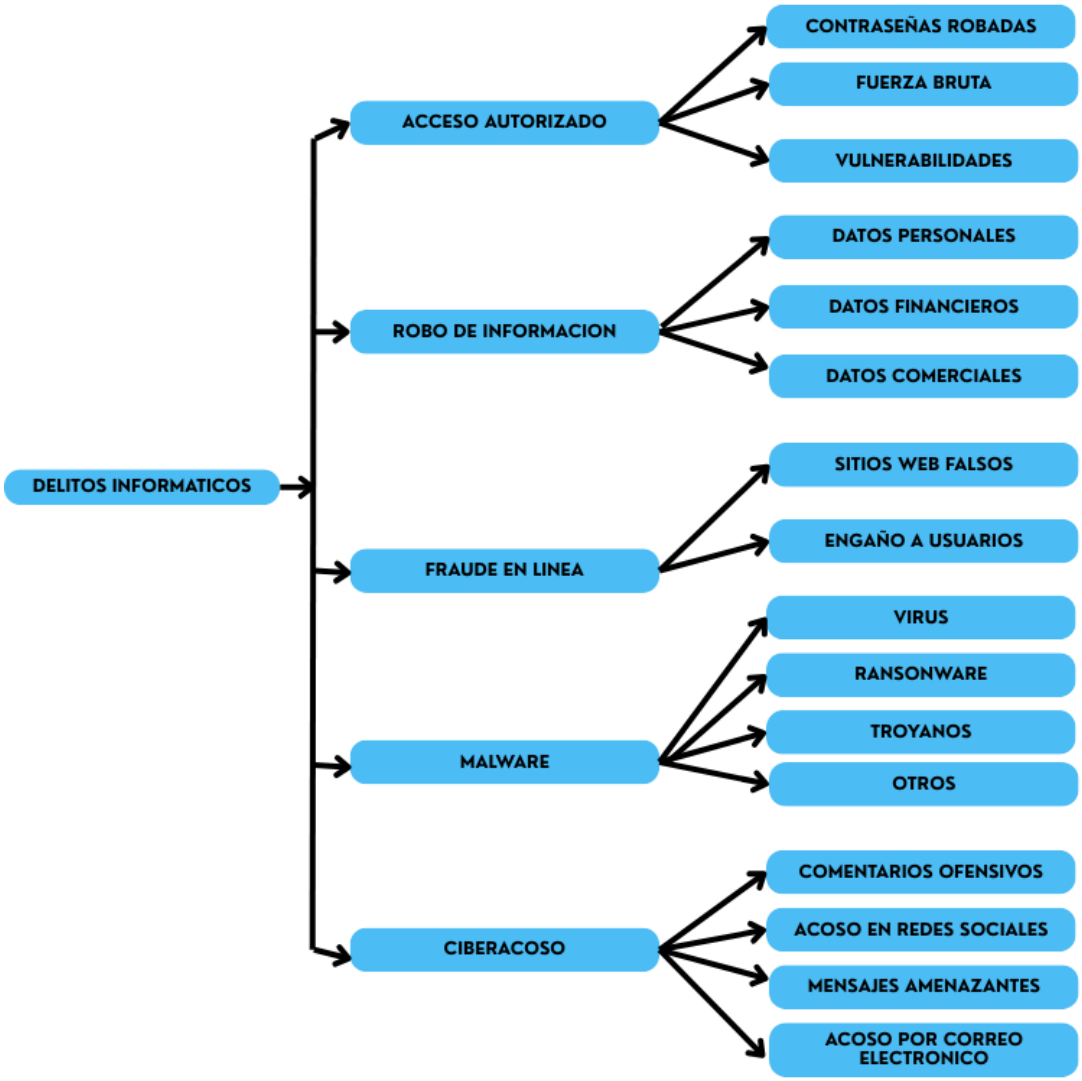
Finalmente, el esquema incluye el **ciberacoso**, entendido como toda conducta de hostigamiento o agresión realizada a través de medios digitales. Esta forma de violencia puede manifestarse en comentarios ofensivos, acoso en redes sociales, acoso mediante correos electrónicos y el envío de mensajes amenazantes, afectando especialmente la dignidad y bienestar psicológico de las víctimas.

Zavala (2018) señala que los delitos informáticos son la forma en que el Estado responde al aumento de la criminalidad en el mundo digital. La Ley N.º 30096 – Ley de Delitos Informáticos, aprobada en 2013, establece diferentes tipos de delitos para proteger la privacidad, la integridad y la disponibilidad de los sistemas y datos digitales. Además, esta norma sigue los lineamientos del Convenio de Budapest, al que Perú pertenece, y que define acciones como el acceso sin permiso, la interceptación de datos, la falsificación digital y el fraude en línea, entre otros.

Martínez (2020) sostiene que incluir estos delitos del Código Penal es un avance normativo importante, ya que permite enfrentar nuevas formas de crimen que no existían en la delincuencia tradicional. Del mismo modo, sostiene que los delitos informáticos deben entenderse no solo desde el enfoque tecnológico, sino también desde la perspectiva jurídico-penal, en tanto que afectan bienes jurídicos clásicos como el patrimonio (fraude), la intimidad (suplantación) y la administración pública (acceso a sistemas estatales). En esa misma línea, Martínez, remarca la necesidad de fiscalías especializadas, capacitadas en informática forense y técnicas de rastreo digital, para que la ley sea realmente efectiva en su aplicación.

Figura 2

Esquema de los delitos informáticos



Fuente: Diagrama extraído del libro Cibercriminalidad y nuevas modalidades delictivas. (Almanza, 2024)

2.1.1.4. El bien jurídico protegido de los delitos informáticos

Según Almanza (2024) delimita los bienes jurídicos vulnerados en diversas categorías siendo los siguientes:

El orden económico, la intimidad, la libertad informática, el honor y la información. Los cuales vamos a explicar detenidamente cada uno de ellos:

- **El orden económico**

Es importante señalar que el orden económico puede verse gravemente alterado por la acción de organizaciones delictivas que vulneran los sistemas digitales, generando una forma de anarquía financiera. Estas conductas no solo afectan el ámbito privado de una empresa, sino que trascienden al plano macrosocial, interfiriendo con las dinámicas y relaciones socioeconómicas generales, pudiendo incluso llegar a comprometer el equilibrio del mercado en su conjunto, como ocurre en situaciones de monopolio absoluto o distorsión del libre comercio.

Asimismo, debe reconocerse que los intereses del Estado, los de los agentes económicos individuales y los de los consumidores confluyen en la protección de un bien jurídico común, como lo es el orden económico. En este sentido, el interés colectivo en el correcto funcionamiento del sistema crediticio y del comercio de capitales ha sido plenamente reconocido por el derecho económico moderno, tanto en el ámbito nacional como internacional, siendo objeto de protección a través de marcos normativos y políticas gubernamentales que buscan preservar la integridad del sistema financiero y el equilibrio del mercado.

- **La intimidad**

El artículo 2, inciso 7, de la Constitución Política del Perú de 1993 protege el derecho al honor, la buena reputación, la privacidad personal y familiar, así como la propia imagen y voz. Esta norma establece un marco legal para resguardar la dignidad de las personas frente a acciones que puedan afectar su vida privada, reputación o entorno familiar, permitiendo una interpretación favorable en el ámbito legal.

En primer lugar, este artículo protege el honor y la buena reputación de los ciudadanos, por ello toda información falsa, ofensiva o difamatoria difundida por cualquier medio debe ser rectificada, garantizando así la integridad moral de las

personas y su reconocimiento social. En segundo lugar, protege el derecho a la intimidad personal y familiar, asegurando que la vida privada esté libre de injerencias no autorizadas. También se prohíbe el uso de la imagen o voz sin consentimiento, salvo excepciones previstas por ley. Si estos derechos son vulnerados, la persona afectada tiene derecho a una rectificación inmediata, gratuita y proporcional al daño causado. Además, quienes cometan actos de difamación, calumnia o invadan la privacidad pueden enfrentar sanciones legales, lo que refuerza la protección constitucional. Esta medida busca reparar el daño causado sin que la persona afectada asuma gastos. Además, el hecho de ejercer estos derechos no evita que los responsables enfrenten sanciones legales. La ley castiga la difamación, la calumnia y la intromisión en la privacidad, lo que demuestra que esta protección constitucional es obligatoria y efectiva.

Ejemplificando esto, supongamos que un canal de televisión difunde una noticia falsa en la que acusa a María Pérez, una ciudadana común, de participar en actividades ilícitas. Al no ser cierta, esta información vulneraría de forma directa su derecho al honor y a la buena reputación. En ese sentido, María tendría pleno derecho a exigir una rectificación pública gratuita y proporcional al daño ocasionado, conforme a lo dispuesto en el artículo 2, inciso 7 de la Constitución. Esta rectificación podría materializarse mediante una disculpa o una nota aclaratoria emitida en el mismo medio de comunicación.

- **La información**

El bien jurídico protegido en materia de información mantiene una relación directa con los delitos informáticos, en tanto estos vulneran la integridad, confidencialidad y disponibilidad de los datos digitales.

Estos delitos tienen como propósito acceder, manipular o destruir información sin autorización, afectando directamente su valor como recurso estratégico y su función dentro del entorno digital. La protección de la información se comprende en tres fases: almacenamiento, tratamiento y transmisión, todas susceptibles de ser vulneradas mediante conductas ilícitas en el ciberespacio.

En primer lugar, los delitos informáticos afectan la seguridad y privacidad de la información cuando los delincuentes ingresan a sistemas o redes sin autorización, exponiendo datos sensibles de personas u organizaciones. Esta acción amenaza la confidencialidad de la información y, por lo tanto, el derecho a la intimidad y protección de datos personales o estratégicos.

En segundo lugar, existe el riesgo de que los datos sean manipulados de forma maliciosa, lo que compromete su veracidad e integridad. Mediante acciones como falsificar registros electrónicos, modificar archivos o difundir información falsa, se puede inducir al error, desinformar o generar perjuicios en distintos ámbitos. Finalmente, los delitos informáticos también pueden destruir o inutilizar información, afectando su disponibilidad. Esto sucede, por ejemplo, con el uso de virus o ransomware, que bloquean, dañan o eliminan datos importantes, ocasionando pérdidas graves para personas o instituciones que dependen de ellos para sus actividades.

- **Libertad informática**

La libertad informática, también llamada *software libre*, es el derecho de los usuarios a usar, estudiar, modificar y compartir programas, garantizando el acceso al conocimiento y a las herramientas tecnológicas. Esta libertad, promovida por Richard Stallman, implica que las personas puedan ejercer control sobre el software y el entorno digital. Otro bien jurídico que resulta gravemente afectado por los delitos informáticos es el honor, entendido como la reputación y la dignidad de las personas. Conductas

como la difamación en redes sociales, el ciberacoso o la divulgación no autorizada de información sensible pueden provocar daños emocionales y sociales significativos, exponiendo aspectos de la vida privada y vulnerando la integridad moral de las víctimas. Estas formas de ciberdelincuencia afectan derechos fundamentales en el entorno digital, lo que hace necesaria una protección legal adecuada y una respuesta oportuna y eficaz por parte del sistema penal.

2.1.1.5. El sujeto activo y pasivo de los delitos informáticos

a) -El sujeto pasivo

Según Jiménez (2017), el sujeto pasivo en la estructura objetiva de la tipicidad penal es el titular del derecho o bien jurídico protegido que ha sido vulnerado por la conducta delictiva. Este puede ser una persona natural, una organización, el Estado o un colectivo. No siempre coincide con la persona sobre la que recae la acción del sujeto activo; por ejemplo, en un homicidio, la víctima es el titular del bien jurídico "vida", mientras que, en un fraude, el engaño puede recaer sobre alguien distinto de quien sufre el perjuicio económico. En conclusión, el sujeto pasivo es quien resulta perjudicado por el delito

En los delitos informáticos, el conocimiento tecnológico del sujeto pasivo es esencial. Las personas o entidades que no tienen conocimientos básicos de informática son mucho más vulnerables a ser víctimas de ciberdelitos. La falta de asesoramiento adecuado en el uso de tecnologías puede llevar a que estas personas sean fácilmente engañadas, como ocurre en la suplantación de identidad cuando se accede a sitios web fraudulentos y se entregan datos personales sensibles. En el ámbito de los delitos informáticos, el sujeto pasivo puede ser una persona natural, una persona jurídica e incluso el propio Estado, tal como lo establecen explícitamente los artículos 7 y 8 de la

ley de delitos informáticos. Gutiérrez Francés señala que las personas jurídicas con un alto potencial económico son, por excelencia, las víctimas más recurrentes de los ilícitos informáticos, siendo la banca, la enseñanza, las instituciones públicas, las industrias de transformación y las aseguradoras los sectores más afectados.

Littejohn Shinder clasifica a las víctimas del cibercrimen en seis categorías principales. Los "nuevos en la red" son los novatos de internet, quienes desconocen las estafas comunes, las medidas de seguridad básicas y las vulnerabilidades del software, lo que los convierte en un objetivo fácil para los ciberdelincuentes. Los "inocentes por naturaleza" incluyen a los más jóvenes y los más viejos, quienes suelen tener una visión distorsionada del mundo y son más confiados, siendo los niños particularmente vulnerables a depredadores como los pedófilos. Los "discapacitados o desaventajados", ya sean mentales o físicos, también son blancos de criminales que los buscan en bases de datos y grupos de apoyo en línea, aprovechando su necesidad de interacción social.

Una cuarta categoría son los "desesperados", personas que buscan soluciones urgentes a necesidades emocionales o físicas (amor, dinero, salvación espiritual), lo que los hace susceptibles a timadores que ofrecen riquezas rápidas, préstamos usureros o empleos fraudulentos. Las "pseudo-víctimas" son aquellos que, por diversas razones, reportan crímenes que no ocurrieron o se presentan como víctimas cuando, en realidad, podrían ser los propios criminales. Finalmente, la categoría de "en el lugar (virtual) adecuado y en el momento adecuado" reconoce que, si bien los depredadores suelen buscar a los más vulnerables, no todas las víctimas son escogidas por su debilidad. Algunos criminales actúan de forma indiscriminada, y en ocasiones, ser víctima es simplemente una cuestión de azar, de estar en el lugar y momento equivocado en el entorno virtual.

b) El sujeto activo

De acuerdo con el libro de Jiménez (2017) en el ámbito delictivo, la presencia de un "sujeto activo" es una exigencia fundamental de la tipicidad, es decir, siempre debe existir un autor o titular de la acción típica. Sin embargo, no todos los sujetos activos poseen las mismas cualidades. Esta diferencia cualitativa se basa en la naturaleza del delito perpetrado o en el *modus operandi*; por ejemplo, un asesino, motivado por el desprecio a la vida humana, difiere significativamente de un estafador, cuya ambición es el lucro. Esta pluralidad de sujetos activos se distingue, por tanto, por la índole de los delitos que cometen.

En este contexto, los perpetradores de delitos informáticos poseen características distintivas. Son individuos con un conocimiento especializado en el uso de la informática, lo que los diferencian de los delincuentes convencionales. A menudo, estos sujetos activos poseen habilidades avanzadas en el manejo de sistemas informáticos y, en ciertos casos, su posición laboral le otorga acceso estratégico a información sensible. No obstante, como señalan Vives Antón y González Cussac, el sujeto activo puede ser tanto una persona legítimamente autorizada para operar un sistema (como operadores o programadores) como un tercero no autorizado que accede a terminales públicas o privadas. En cualquier caso, el elemento común es que deben poseer los conocimientos o las condiciones técnicas suficientes para manipular la informática. Históricamente, la percepción del sujeto activo en delitos informáticos evolucionó. Inicialmente, impulsada por los primeros casos de estudiantes estadounidenses, se les consideraba adolescentes de clase media, inofensivos, con un coeficiente intelectual alto y sin una plena conciencia de la ilicitud de sus actos, actuando por curiosidad, desafío o un sentido de superioridad. Sin embargo, con el avance tecnológico y la consolidación de la sociedad digital, esta visión se transformó en un mito. La imagen del ciberdelincuente cambió hacia individuos motivados por el

lucro o el deseo de causar daño, que no necesariamente poseían una inteligencia superior, sino más bien conocimientos técnicos suficientes, y podían provenir de cualquier estrato social.

A pesar de esta evolución, parte de la doctrina no comparte la idea de un nivel intelectual diferenciado para los ciberdelincuentes. Estos expertos sostienen que los sujetos activos son personas listas, decididas y dispuestas a aceptar retos tecnológicos, con similitudes a los perpetradores de "delitos de cuello blanco" –caracterizados por su estatus social y la ausencia de motivaciones como la pobreza o la falta de educación. Autores como Tiedemann y Bramont-Arias señalan que, en la actualidad, los autores son usuarios comunes que no requieren de vastos conocimientos informáticos para cometer conductas delictivas en este ámbito, lo que simplifica la comisión de este tipo de crímenes.

2.1.1.6. Diligencias Preliminares en delitos informáticos.

Las fases iniciales marcan el comienzo de la investigación, y nuestro Código Procesal Penal, en su artículo 329, autoriza al fiscal a iniciar las acciones investigativas que considere necesarias al tener conocimiento de un hecho delictivo.

Así, Velarde (2021) señala que esta investigación abarca los primeros pasos de toda investigación penal: las primeras declaraciones, actuaciones investigatorias y aseguramiento de los primeros elementos de prueba; los que serán relevantes para la formalización o el sobreseimiento de la causa.

En esta misma idea, César San Martín (2017) opina que consiste en la búsqueda de un conjunto de elementos que permitan el descubrimiento de la verdad sobre hechos que sean considerados como conductas delictivas.

En relación con lo mencionado, se puede añadir que en la investigación inicial se llevan a cabo todas las acciones urgentes e inaplazables dirigidas a verificar los hechos reportados y establecer si son criminales. Además, se realiza una indagación con el objetivo de obtener pruebas, tanto a favor como en contra, que ayuden al Fiscal a decidir si presenta o no la acusación.

La rapidez en la investigación de un delito es fundamental, ya que el tiempo transcurrido puede dificultar la obtención de pruebas. La investigación reactiva comienza con la presentación de una denuncia, lo que alerta a las autoridades sobre hechos presuntamente delictivos y activas estrategias legales para la persecución penal. Este tipo de investigación es especialmente importante en casos evidentes de muerte violenta o agresiones con signos de resistencia, donde se requiere la intervención de expertos para identificar a los sospechosos. En otros casos, cuando no se puede determinar de inmediato si ocurrió un delito, la investigación reactiva busca establecer la existencia de un hecho delictivo y quiénes podrían ser responsables. Por su parte, la investigación proactiva no parte de una denuncia o sospecha inicial, sino que se desarrolla mediante un análisis sistemático para generar indicios de posibles delitos.

Este enfoque, que debe estar respaldado por políticas públicas, se basa en un análisis tradicional para tipificar el delito, identificando patrones comunes y analizando causas directas e inmediatas. Su objetivo es encontrar información relevante que permita esclarecer presuntos delitos y prevenir futuros incidentes delictivos. Este proceso incluye examinar el contexto de los delitos, como el tipo y valor de los objetos robados y los posibles mercados para los bienes sustraídos, con el fin de desarrollar estrategias y políticas preventivas, involucrando directamente a operadores judiciales. La investigación preliminar se refiere al período inicial en que se indaga sobre posibles delitos que afectan derechos personales o colectivos, sin asumir cargos contra los implicados y respetando la presunción de inocencia. Durante esta etapa, se busca recopilar pruebas, como testimonios y declaraciones de testigos, que permitan confirmar

o descartar las sospechas iniciales. La jurisprudencia internacional, especialmente del Tribunal Europeo de Derechos Humanos, establece que los tribunales deben garantizar un “plazo razonable” según la complejidad del caso, la conducta de los solicitantes y las acciones de las autoridades. En la actualidad, asegurar un plazo razonable requiere supervisión constante del proceso para proteger los derechos de los imputados. El Código Procesal Penal (CPP) de 2004 implementó un sistema de control de plazos en las diligencias preliminares, buscando que la investigación se realice en un tiempo adecuado y orientada a la búsqueda de la verdad por parte de los operadores judiciales.

Frank Almanza (2024) presenta un esquema de las diligencias preliminares en delitos informáticos.

a) Las declaraciones son importantes, ya que, a través de los testimonios detallados de testigos o víctimas, se obtiene una aproximación de lo ocurrido, proporcionando datos sobre la naturaleza del incidente, el modus operandi percibido y posibles sospechosos o pistas esenciales.

b) Paralelamente, el Informe Técnico es una herramienta indispensable, con mayor relevancia en la criminalidad informática. Este análisis pericial, permite establecer hipótesis sólidas sobre cómo se ejecutó el delito y las herramientas o técnicas empleadas, también permite la ubicación y captura de los infractores. Este informe permite rastrear huellas digitales, direcciones IP, metadatos y otros indicios tecnológicos que conducen al paradero de los perpetradores.

c) La recolección de pruebas es fundamental en cualquier proceso legal, y en los delitos informáticos resulta especialmente compleja. Consiste en obtener y asegurar elementos, tanto digitales como físicos, que demuestren la comisión del delito. Esto incluye dispositivos electrónicos, discos duros, archivos digitales, registros de actividad y

comunicaciones electrónicas, los cuales deben manejarse siguiendo estrictos protocolos de cadena de custodia para garantizar su integridad y validez en un posible juicio.

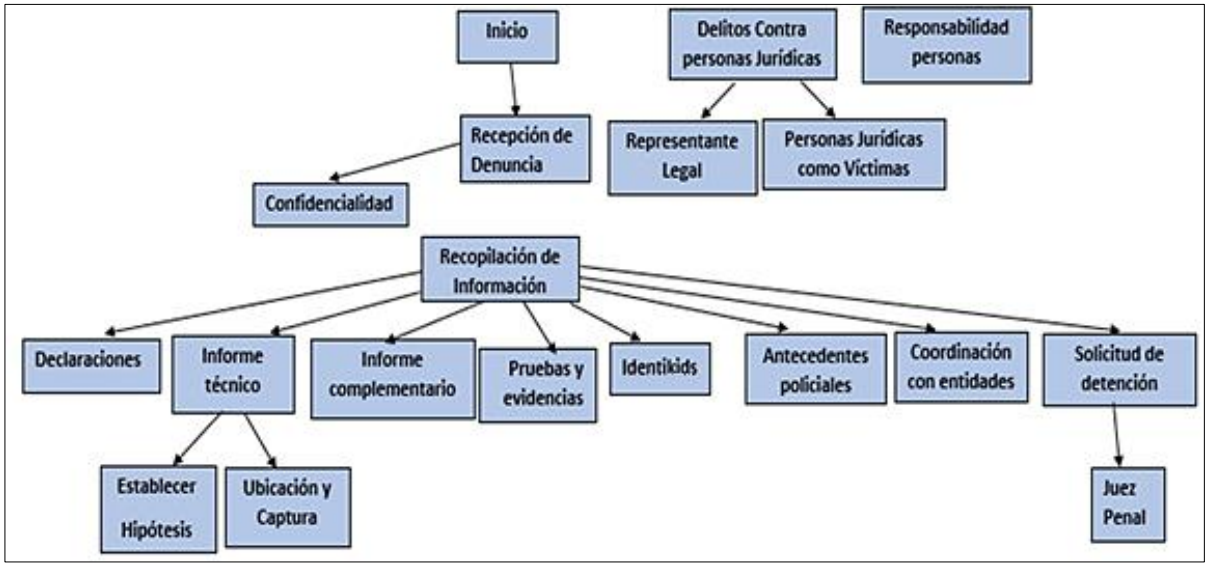
d) Cuando es difícil identificar directamente al sospechoso, la creación de Identikits resulta útil. Aunque normalmente se asocia a delitos presenciales, en el caso de los ciberdelitos puede implicar la elaboración de perfiles de posibles responsables a partir de su comportamiento en línea, el lenguaje que usan o los patrones de sus ataques, lo que ayuda a las autoridades a dirigir mejor la investigación.

e) La revisión de antecedentes policiales es otra diligencia importante que permite verificar si los sospechosos o incluso los testigos cuentan con antecedentes delictivos. Esta información es útil para identificar patrones de conducta, evaluar la posibilidad de reincidencia y detectar posibles vínculos con otros delitos, lo que contribuye a completar el perfil del caso.

f) Finalmente, la coordinación con entidades subraya la naturaleza interconectada de la investigación de delitos informáticos. Dada la complejidad y la naturaleza transfronteriza que a menudo presentan es imperativo establecer una colaboración estrecha con otras instituciones, tanto nacionales como internacionales, así como con empresas de tecnología, proveedores de servicios de internet, o incluso organismos financieros. Esta cooperación permite el intercambio de información, la obtención de datos sensibles y el acceso a recursos especializados que son inalcanzables para una única entidad investigadora.

Figura 3

Actividades probatorias



Fuente: Diagrama extraído del libro Criminalidad y Nuevas Modalidades Delictivas (Almanza, 2024)

2.1.1.7 Actividades Probatorias.

Esta es la etapa inicial para determinar si un hecho constituye un delito. En esta fase, el Fiscal lidera el proceso, dirigiendo personalmente o junto con la Policía las acciones urgentes, necesarias e inaplazables para comprobar si realmente ocurrió un ilícito. Además, el Fiscal debe asegurar los elementos materiales del delito, identificar a las personas involucradas y garantizar su participación en el proceso penal.

A. El levantamiento del secreto de las comunicaciones.

Se ha convertido en una herramienta clave para investigar delitos complejos, especialmente los informáticos, que dejan rastros digitales. Esta medida permite acceder a correos electrónicos, mensajes de texto, registros de llamadas o datos de navegación, lo que implica una afectación a derechos como la privacidad y la intimidad. Por ello, su uso está estrictamente regulado y debe cumplir con principios de legalidad, proporcionalidad y necesidad, requiriendo siempre autorización judicial motivada (Villavicencio, 2012). La

creciente sofisticación de la ciberdelincuencia ha llevado a que los sistemas jurídicos adapten sus normas para mejorar la recolección de pruebas digitales, siempre bajo control de la autoridad judicial.

B. Incautaciones y Allanamientos

Por otro lado, las incautaciones y allanamientos son medidas clave en la investigación, ya que permiten obtener pruebas que respalden la teoría del delito presentada por el Ministerio Público. Estas diligencias facilitan el acceso a lugares cerrados, como domicilios o locales, para buscar y asegurar bienes, documentos o instrumentos directamente relacionados con la comisión del delito. Su ejecución está regulada en el Código Procesal Penal peruano, específicamente en los artículos 210 al 218, y requiere autorización judicial previa, salvo en casos de flagrancia o peligro inminente.

Desde un punto de vista probatorio, estas medidas son esenciales para reconstruir materialmente los hechos. El hallazgo de armas, droga, documentos falsificados, dinero en efectivo o aparatos electrónicos puede constituir prueba directa del delito o, al menos, un indicio razonable que respalde la hipótesis delictiva. Además, permiten vincular físicamente al imputado con la escena del crimen o con elementos clave del hecho, lo cual contribuye a probar aspectos como la tipicidad, el dolo, e incluso la participación criminal

C. Declaraciones testimoniales y colaboradores eficaces

Por otra parte, otra medida que considero eficaz, son las declaraciones testimoniales y los testimonios de colaboradores eficaces constituyen medios probatorios personales de alta relevancia en el proceso penal. De ese modo, a través del testimonio, se busca reconstruir verbalmente los hechos delictivos mediante la percepción directa o indirecta que una persona ha tenido sobre el suceso. En el caso del colaborador eficaz, este es un imputado que brinda información útil, veraz y comprobable a cambio de beneficios procesales, de conformidad con

lo regulado en la Ley N.º 27378 y su modificatoria, el Decreto Legislativo N.º 1301 en el contexto peruano. Ambos medios de prueba resultan claves para fortalecer la teoría del delito formulada por el Ministerio Público, en particular respecto a la participación, el dolo, la planificación y la existencia misma del hecho punible.

Del mismo modo, es importante recalcar la relevancia del testimonio de terceros (testigos) puede ser directo o indirecto, y su fuerza probatoria dependerá de su coherencia interna, la ausencia de contradicciones, el modo en que fue obtenido y su corroboración con otros medios probatorios. Por su parte, la declaración del colaborador eficaz tiene un valor especial en la investigación de delitos complejos, como crimen organizado, corrupción o lavado de activos, ya que permite conocer desde el interior cómo se ejecutaron los actos delictivos, quiénes participaron y cómo se distribuyeron roles, elementos que muchas veces no pueden obtenerse mediante evidencia física.

En consecuencia, de acuerdo con la gravedad del hecho se pueden emplear diversos mecanismos para garantizar una adecuada recolección de datos. En esa línea, los peritajes técnicos constituyen uno de los medios probatorios más importantes en el proceso penal moderno, especialmente en la investigación de delitos complejos o que requieren conocimientos especializados para ser comprendidos por los jueces y fiscales. Este tipo de prueba es aportada por peritos, profesionales con formación técnica o científica, que analizan e interpretan elementos de prueba desde una perspectiva objetiva, con base en principios de su especialidad.

D. Los peritajes

Los peritajes pueden ser de muy diversa índole. Los peritajes informáticos permiten analizar dispositivos electrónicos, recuperar archivos, rastrear comunicaciones digitales o comprobar manipulación de sistemas. Mientras que los peritajes balísticos determinan el tipo

de arma usada, trayectoria de proyectiles, distancia de disparo, entre otros aspectos. Por su parte, los peritajes contables o financieros se emplean para rastrear el movimiento de dinero, detectar desbalances patrimoniales o estructuras de lavado de activos. Cada uno de estos informes refuerza la teoría del delito aportando conocimiento técnico que permite acreditar la existencia del hecho, su modo de ejecución y la participación de los imputados.

Desde la doctrina, Taruffo (2009), afirma que el peritaje es un instrumento esencial para establecer el nexo causal entre el comportamiento del imputado y el resultado típico, especialmente en delitos donde los indicios materiales requieren interpretación especializada. Por su parte, Aroca (2010) sostiene que el perito es un "auxiliar del juez", cuya función es ofrecer claridad técnica en aquellos aspectos que escapan al conocimiento jurídico. En ese sentido, el dictamen pericial no puede ser valorado de forma aislada, sino en conjunto con los demás medios probatorios, aunque en muchos casos adquiere relevancia decisiva.

2.1.1.8. Actividad probatoria realizada por la Policía.

En el contexto de un hecho ilícito, la Policía realiza la primera intervención. Esto incluye acudir al lugar del incidente, redactar un informe sobre lo encontrado, como objetos y personas presentes, y posteriormente informar al Ministerio Público. El Ministerio Público puede delegar tareas a la Policía o iniciar investigaciones de manera independiente. Según la Ley N° 27934, la Policía debe llevar a cabo las siguientes acciones: primero, recibir y documentar la denuncia en un informe; segundo, proteger el lugar del crimen para preservar las pruebas; tercero, brindar asistencia a las personas afectadas y registrar en el informe a los testigos presentes; cuarto, recoger y examinar los objetos relacionados con el delito; quinto, realizar diligencias para identificar al autor del delito; sexto, tomar declaraciones de testigos; y séptimo, arrestar a los presuntos culpables, respetando sus derechos, incluyendo su integridad física y mental y el derecho a una defensa legal.

2.1.1.9. Actividad probatoria realizada por la Fiscalía.

Posteriormente, el Fiscal evaluará la denuncia para determinar si el hecho califica como delito. Si el Fiscal concluye que no hay base para una acción penal, puede ordenar el archivo de lo actuado. De acuerdo con la Ley N° 27934, el Fiscal posee ciertas atribuciones, como ordenar la detención preliminar del presunto autor por hasta 24 horas, incluso si el delito no se cometió en flagrancia, siempre que se solicite de manera fundamentada y escrita al Juez. Además, puede solicitar medidas coercitivas cuando sea necesario, independientemente de la flagrancia, cumpliendo con los requisitos establecidos en los artículos 135 y 143 del Código Procesal Penal.

Según el Informe del Ministerio Público (2021), una de las principales dificultades que enfrentan los Fiscales en los casos de delitos informáticos es la etapa preliminar. La obtención de información de medios electrónicos, direcciones IP o la apertura de teléfonos bloqueados resulta especialmente complicada, y si no se logra obtener estos datos, se dificulta la localización de los autores del delito. El informe también indica que muchas denuncias se archivan debido a la imposibilidad de identificar al sujeto activo, un problema agravado por la falta de unidades tecnológicas avanzadas dentro de la Policía Nacional. La ausencia de peritos informáticos contribuye a una investigación menos eficiente y más prolongada. (Gómez, 2024).

2.1.1.10. La Unidad Fiscal Especializada en Ciberdelincuencia

Durante 2020, el Ministerio Público de Perú estableció una comisión para evaluar la creación de una unidad especializada en ciberdelincuencia, esta unidad se ocupa de dictar lineamientos, unificar criterios y apoyar investigaciones relacionadas con delitos informáticos y fraudes que involucren información digital.

En junio de 2021, se creó la Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro, con competencia en 16 distritos, compuesta por un fiscal superior y varios

fiscales adjuntos. Sin embargo, existen importantes obstáculos como la falta de respuesta oportuna de las entidades bancarias y las empresas de telecomunicaciones ante las solicitudes judiciales. Algunas de estas empresas no cumplen con la obligación de conservar datos durante el tiempo requerido, dificultando la identificación y localización en investigaciones de ciberdelitos. Esta problemática está regulada por el Decreto Legislativo N° 1182, publicado en 2015, que establece cómo deben manejarse los datos de telecomunicaciones para combatir delitos. Es por ello, la relevancia de esta entidad pues la Red de fiscales en Ciberdelincuencia garantiza privacidad y anonimato frente a amenazas digitales.

2.1.2. Ciberdelincuencia y los delitos con relación a las Tecnologías de la información

El uso de tecnologías de la información y la comunicación (TIC) facilita actos delictivos tradicionales. Aunque estos delitos pueden realizarse sin tecnología, las TIC amplifican su alcance, es crucial distinguir entre delitos tradicionales y ciberdelitos; la simple utilización de tecnología no convierte uno en el otro. Reconocer los tipos penales clásicos que se perfeccionan con el uso tecnológico es fundamental para enfrentar los desafíos del ciberespacio, que incluyen: El uso de tecnologías de la información y la comunicación (TIC) facilita actos delictivos, aunque estos delitos pueden realizarse sin tecnología, las TIC amplifican su alcance, es por ello que, se debe reconocer los tipos penales clásicos que se perfeccionan con el uso tecnológico es fundamental para enfrentar los desafíos del ciberespacio, que incluyen: anonimato, inmediatez, masividad, internacionalidad y dificultades en la obtención de evidencia digital, esto es esencial para desarrollar estrategias efectivas de lucha contra estos delitos. Como señala Felipe Villavicencio (2014), la investigación inicial implica llevar a cabo todas las acciones urgentes e inaplazables para verificar los hechos denunciados y determinar si constituyen un delito. Además, se realiza una indagación para obtener pruebas, tanto a favor como en contra, que ayuden al Fiscal a decidir si presenta o no una acusación.

En atención a lo citado, las TID no convierte a un delito tradicional en ciberdelito, pero si pueden facilitar, utilizar y fomentar la comisión de los delitos aprovechándose de la existencia de las TID.

Siguiendo esa línea, la Fiscalía de Lima Centro posee una estructura organizativa especialmente diseñada para garantizar la eficacia del sistema de justicia penal en los diversos distritos que conforman su jurisdicción. Dicha fiscalía está conformada por fiscales superiores, quienes representan la máxima autoridad dentro del distrito fiscal y tienen la responsabilidad de supervisar, coordinar y velar por el cumplimiento de las funciones constitucionales y legales del Ministerio Público. Asimismo, su estructura incluye a fiscales provinciales, fiscales adjuntos provinciales y al personal administrativo, quienes, en conjunto, se encargan de ejecutar labores de investigación penal, prevención del delito y representación del Estado ante los órganos jurisdiccionales.

La Fiscalía de Lima Centro abarca 16 distritos, entre ellos: Cercado de Lima, Breña, Rímac, Jesús María, La Victoria, San Luis, Santiago de Surco, Barranco, Miraflores, San Miguel, Surquillo, San Borja, entre otros. Cada uno de estos distritos cuenta con despachos fiscales descentralizados que tienen como función principal velar por la seguridad ciudadana, mediante la recepción de denuncias, la investigación del delito, la protección de las víctimas y la persecución penal de los autores de los hechos delictivos.

En este contexto, y considerando el aumento de las conductas delictivas cometidas a través de medios tecnológicos, se hace relevante la labor de las Fiscalías Especializadas en Ciberdelito, las cuales, aunque centralizadas en algunos puntos del país, extienden su competencia funcional a nivel nacional. Estas fiscalías tienen como función principal investigar delitos informáticos y otros cometidos mediante el uso indebido de tecnologías de la información, tales como el fraude informático, suplantación de identidad, acoso digital,

pornografía infantil en línea, violación de la intimidad, estafas electrónicas, acceso ilícito a sistemas o bases de datos, entre otros.

Por tanto, la Fiscalía de Lima Centro no solo cumple funciones esenciales en la persecución penal ordinaria dentro de su jurisdicción territorial, sino que también coopera con fiscalías especializadas cuando se presentan delitos cibernéticos, fortaleciendo así la respuesta institucional frente a nuevas formas de criminalidad, y reafirmando el compromiso del Ministerio Público con la defensa de la legalidad, los derechos fundamentales y la seguridad pública.

2.1.2.1 Impacto de la ciberdelincuencia.

La ciberdelincuencia en el Perú ha tenido un impacto amplio y sobre todo negativo para individuos como para las entidades, este impacto afecta no solo a las personas con robos de identidad, estafas sino también a las empresas quienes sufren pérdidas financieras y daños a la reputación.

En este contexto, los delitos cibernéticos han crecido considerablemente, con pérdidas económicas que subieron de 3 billones de dólares en 2015 a 6 billones en 2021. Esto, según Interpol, equivale al producto interno bruto de una de las principales economías globales. Este fenómeno no solo implica un costo económico, sino que también afecta la confianza de los usuarios en la economía digital. Menos de la mitad de los internautas creen que la tecnología puede mejorar sus vidas, principalmente por preocupaciones sobre la privacidad de sus datos.

2.1.2.2 Factores que dificultan la persecución eficaz de los delitos informáticos. Como bien ya tenemos noción, el Nuevo Código Procesal Penal establece tres etapas del proceso: preparatoria, intermedia y juicio oral. La etapa preparatoria es crucial, ya que recopila elementos que dan fundamento a la investigación y convicción sobre la conducta delictiva, divida en la etapa de diligencias preliminares y formalización de la investigación, sin embargo,

estas etapas pueden verse obstaculizada por factores que afectan la correcta investigación del delito, o en este caso, logrando una mala persecución del delito.

Existen factores que impiden una correcta persecución eficaz de delito, pues esta mala persecución se refiere a la ineficiencia de las investigaciones fiscales que no logran recabar pruebas suficientes.

Estas refieren a las circunstancias que surgen en las investigaciones preliminares y que constituyen a un resultado deficiente con respecto a la persecución del delito podríamos decir que estas investigaciones pueden tener vicios omisiones o defectos en sus diligencias originando que la persecución del delito sea ineficaz.

Esto resulta en una falta de protección a los derechos de la víctima y afecta negativamente la productividad del Ministerio Público, debido a diversos factores que interfieren en estas investigaciones, logrando así una deficiente persecución de los delitos.

2.1.2.3. Anonimato del agente.

En relación con la investigación efectiva de los crímenes cibernéticos, esta se dificulta por varios motivos, siendo uno de ellos el anonimato del perpetrador. Dicho anonimato es posible gracias a métodos de encriptación que ocultan la identidad del infractor, además del uso de plataformas digitales que permiten a los criminales en línea ejecutar sus acciones.

Tal como se indicó previamente, este anonimato complica la indagación y el seguimiento de los delitos, afectando a todos los crímenes cibernéticos, dado que la información que ayude a identificar al autor es escasa.

2.1.2.4. La falta de colaboración de la víctima en la investigación de los delitos informáticos.

Un factor que reduce la efectividad en la lucha contra el delito informático es que quien denuncia no colabora lo suficiente para esclarecer los hechos y, además, posee un bajo nivel

de conocimiento sobre seguridad digital. Esto implica que, si bien la víctima aporta información crucial en estos delitos, la constante aparición de nuevas Tecnologías de la Información y Comunicación (TIC) facilita identificar las diversas modalidades en que ocurren estos crímenes y los derechos que resultan afectados. Según Espinoza (2022) el desconocimiento de los delitos informáticos genera una frustración en los denunciantes al tener la dificultad de identificar al autor eso conlleva a un sentimiento de injusticia que ocasiona el desistimiento de continuar colaborando con la investigación. (p.68).

Por otro lado, la conducta que tiene la víctima frente a esta situación, refiriendo primero que existe primordialmente una afectación económica, también psicológica y patrimonial, además de que se requiere necesariamente que el hombre se identifique y por medio de ello se le reconozca en la sociedad, de la misma forma en el ámbito informático el sujeto mantiene una identidad propia, debido a que por medio de la informática la persona va a desarrollar su vida privada, su vida económica y también social, bajo este criterio se puede decir que las semejanzas son importantes; cabe mencionar que la persona siempre mantiene su aspecto económico dentro de la informática, todo ello a través de las cuentas bancarias y de los servicios financieros, el cual priva a la persona en la acumulación de información social por medio de las redes, por lo que la vulneración a esta institución lesionará de gravedad a la persona, y merma su economía, dañando la estabilidad de la persona tanto emocionalmente como psicológicamente ya que compromete información reservada.

Por consiguiente, las personas afectadas por delitos informáticos son aquellas cuya información personal ha sido comprometida. Dado que la autoridad enfrenta dificultades para actuar de manera rápida debido a la alta carga de casos complejos, se ha podido observar que estos delitos causan daños al honor, la imagen pública y la integridad de las víctimas, lo cual indica una alteración en su estabilidad psicológica. Los ataques de pánico y la ansiedad son manifestaciones comunes en estos casos (Usaqui, 2022).

2.1.2.5. Ausencia de peritos en materia de delitos informáticos

La falta de expertos en delitos digitales dificulta la persecución efectiva del crimen. Rayón Ballesteros y Gómez Hernández (2014) señalan que la naturaleza cambiante de las pruebas electrónicas exige procedimientos que garanticen su integridad. Por ello, el autor argumenta que es crucial capacitar a los abogados en delitos informáticos para asegurar que estas pruebas sean válidas en un juicio. En ese sentido, el perito informático es fundamental en la investigación de fraudes informáticos, encargándose de identificar direcciones IP de dispositivos, sigue procedimientos estandarizados en la gestión de evidencias digitales, desde su identificación hasta la presentación de informes, utilizando software y hardware reconocidos para colaborar en causas judiciales.

En esa misma línea, es importante señalar que la capacidad del Ministerio Público para investigar eficazmente los delitos informáticos se ve considerablemente mermada por la ausencia o insuficiencia de nuevas tecnologías. Aunque se han realizado esfuerzos por modernizar el sistema de justicia, como la reciente Ley N° 32374 que incorpora el uso de tecnología digital en la remisión de la carpeta fiscal y otras diligencias (Ticse Baquerizo, 2025), la realidad sobre el terreno muestra que persisten significativas brechas.

Uno de los principales problemas radica en la falta de infraestructura tecnológica adecuada y la escasez de implementos informáticos de vanguardia. La investigación de delitos en el ciberespacio exige herramientas forenses especializadas, software de análisis de datos masivos y equipos capaces de procesar y resguardar evidencia digital de manera segura y confiable. Como señalan estudios recientes, el Perú aún carece de gran parte de la tecnología necesaria para investigar eficazmente esta índole de delitos, lo que se traduce en serias limitaciones de recursos tecnológicos para las fiscalías.

Además de la infraestructura, la capacitación del personal fiscal y policial en el uso de estas tecnologías es un desafío constante. A pesar de la creación de unidades especializadas como la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público, y la implementación de laboratorios y plataformas específicas (Ministerio Público, 2021), la constante evolución de las técnicas delictivas informáticas exige una actualización y formación permanente que muchas veces no se logra cubrir de manera integral. La impunidad en los delitos informáticos se debe, en parte, al hecho de que "es imposible individualizar al criminal debido a la naturaleza anónima de estos delitos y a que ocurren en el ciberespacio"; además, si no se logra identificar a los culpables durante las diligencias preliminares, la persecución efectiva tiende a desvanecerse. (Rosales Medina, 2024).

En este sentido, la ausencia de una inversión sostenida en tecnología y la dificultad para mantenerse al día con las innovaciones que los ciberdelincuentes utilizan, limita la capacidad del Estado para hacer frente a una criminalidad que es cada vez más compleja y globalizada. Como lo menciona un estudio del Poder Judicial, "la impunidad en los delitos informáticos [es] una problemática de poco interés para legisladores, jueces y fiscales", lo cual subraya la necesidad de un mayor compromiso para dotar a las instituciones de justicia con los recursos tecnológicos y humanos necesarios para combatir eficazmente el cibercrimen.

2.1.2.6. La Necesidad de contar con órganos jurisdiccionales capacitados en investigación criminal de delitos informáticos

La falta de conocimiento de los fiscales sobre las diligencias en investigaciones de los delitos informáticos provoca ineficiencia en la persecución de los delitos informáticos, siendo esencial que los fiscales comprendan procedimientos de informática, como la identificación de IP, la obtención de información de correos electrónicos y la recuperación de archivos eliminados. Esto les permitirá formular requerimientos adecuados y manejar evidencia digital en las investigaciones.

Según Ballesteros y Gómez (2014), la delincuencia en línea exige planes que integren el trabajo de inteligencia de los investigadores. Sin embargo, también es crucial obtener y preservar las pruebas de tal manera que conserven su validez. Esto es fundamental porque el poder judicial examinará estas pruebas minuciosamente, ya que deben demostrar la comisión de un delito cibernético.

Es así como, surge la necesidad de contar con fiscales capacitados en materia de delitos informáticos en vista a que el representante del MP quien conduce la investigación en compañía de la Policía Nacional, es crucial que estén capacitados para centrarse en el análisis de la evidencia digital y requieran información relevante de proveedores de servicios informáticos y redes sociales.

2.1.2.7. Cooperación Internacional para perseguir el Delito

Las instituciones del sistema bancario son esenciales para detectar a quienes cometen fraudes digitales, dado que tienen datos sobre los dueños de las cuentas. De acuerdo con el artículo 235 del Código Penal Procesal y la Resolución 4933-2014 emitida por la Fiscalía, se establece un protocolo que permite a los fiscales solicitar información a las entidades ante operaciones financieras sospechosas, el fiscal puede pedir el levantamiento del secreto bancario al juez, con un plazo de respuesta de treinta días, que resulta excesivo para investigaciones urgentes.

La falta de colaboración con las instituciones del sistema financiero también es un factor. Esta colaboración permitiría que estas ofrezcan información crucial para identificar a los implicados sin revelar detalles que pongan en riesgo el secreto bancario. Según Flores (2014), a menudo, en el proceso de investigación, cuando las entidades financieras se negaban a dar los nombres de los dueños de las cuentas que recibieron fondos no permitidos, se veían forzados a realizar depósitos de pequeñas cantidades en esas cuentas identificadas, con el fin

de averiguar el nombre de los titulares y así avanzar con la investigación. Esta situación, según su opinión, podría evitarse si las instituciones financieras proporcionan esta información como resultado de un acuerdo de cooperación establecido. (p. 70).

Por otro lado, el concepto de fraude se refiere a la introducción de datos falsos o engañosos, también conocidos como “data diddling”, según lo tipificado por el código penal. Esto implica la manipulación de datos en los sistemas informáticos de las empresas para llevar a cabo operaciones fraudulentas sin el conocimiento de estas. Este tipo de fraude se ha convertido en uno de los delitos informáticos más comunes debido a que es relativamente sencillo de ejecutar desde el exterior, sin necesidad de acceso directo a los archivos de la empresa. Sin embargo, aunque estos fraudes suelen ser detectados eventualmente, la reacción suele ser tardía. En este contexto, el fraude se ha convertido en una técnica ampliamente utilizada por los delincuentes, dado que existen numerosos sistemas operativos capaces de vulnerar la seguridad de las empresas.

2.1.2.8. Factores Clave en la Investigación de Ciberdelitos y su Enlace con la Cooperación Internacional

De acuerdo con el diagrama extraído del autor Frank Almanza (2024) se puede evidenciar que el gráfico posee componentes fundamentales que intervienen en el proceso de investigación de ciberdelitos: la localización y geolocalización, la investigación técnica del delito y la colaboración internacional. Siendo así que dichos elementos permiten una actuación más eficaz frente a crímenes informáticos, que suelen tener características transnacionales y complejas.

De ese modo, en primer lugar, la localización y geolocalización constituyen herramientas indispensables para rastrear la ubicación de los actores involucrados en

actividades delictivas en entornos digitales. Para ello, se requiere el acceso a datos precisos de localización y el uso de plataformas virtuales que permitan la trazabilidad. Asimismo, se enfatiza la necesidad de contar con recursos asignados específicamente a esta función, lo cual contribuye a establecer una ubicación referencial útil para orientar las acciones operativas de captura o vigilancia.

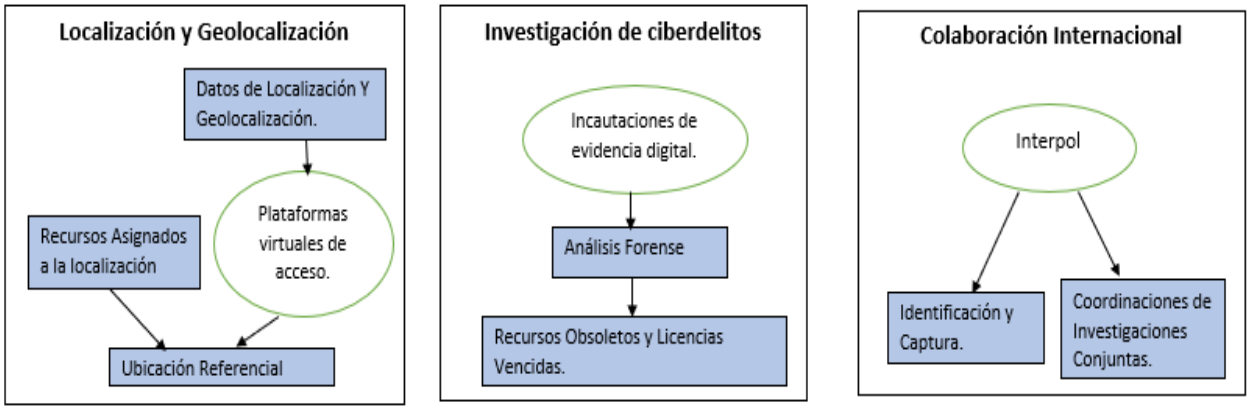
En segundo lugar, la investigación de ciberdelitos se inicia generalmente con la incautación de evidencia digital, como dispositivos electrónicos, discos duros o archivos en la nube. Esta información es luego sometida a un análisis forense especializado, que permite identificar patrones de conducta, conexiones, archivos manipulados o comunicaciones relevantes. No obstante, el esquema advierte una dificultad común: el uso de recursos obsoletos o con licencias vencidas, lo cual puede limitar la calidad y fiabilidad del análisis pericial, afectando negativamente el curso de la investigación.

Finalmente, el componente de colaboración internacional es esencial debido a que muchos ciberdelitos involucran redes que operan desde distintos países. En este contexto, organismos como Interpol juegan un papel crucial al facilitar la identificación y captura de sospechosos en el extranjero, así como la coordinación de investigaciones conjuntas entre autoridades de diferentes jurisdicciones.

Esta cooperación internacional permite superar las limitaciones territoriales del derecho penal tradicional, fortaleciendo así la respuesta frente al crimen organizado en entornos digitales.

Figura 4

Herramientas y Procedimientos en la Investigación de Delitos Digitales



Fuente: Diagrama extraído del libro Criminalidad y Nuevas Modalidades Delictivas (Almanza, 2024)

2.1.2.9. Necesidad de realizar una correcta percusión eficaz de los delitos informáticos

La necesidad que existe de realizar una correcta persecución eficaz se fundamenta en la importancia de mantener el orden social disuadir la delincuencia, sobre todo garantizar la justicia y fortalecer el estado de derecho, sin embargo, la persecución eficaz también es importante para perseguir correctamente del delito, evitar la impunidad y garantizar los derechos de las víctimas.

2.1.3.0 Evitar impunidad

La impunidad se define como la ausencia de sanción por un acto delictivo, siendo "impune" aquello que queda sin castigo. La impunidad se refiere a la ausencia de penalización, permitiendo que un delincuente quede exento de una pena por el delito cometido. De este modo, se sostiene que la impunidad es una de las causas más frecuentes en este contexto, siendo una de las situaciones que más afecta la percepción colectiva al no sancionar a los verdaderos responsables de los delitos.

En ciertos casos, la persecución recae sobre figuras públicas, a menudo por motivos políticos, donde se evidencian abusos por parte de organismos estatales. En estos escenarios,

se limita la libertad, se somete a la prensa a una censura total, se manipulan los tribunales y el poder se concentra en una minoría que se mantiene mediante coacción, miedo y una cobardía generalizada.

En relación con la impunidad en la administración de justicia y su vínculo con los delitos informáticos, se sostiene que esta se encuentra en un estado de deterioro debido a la falta de comprensión por parte de los legisladores de que las reglas diseñadas para el ámbito físico no son aplicables de manera efectiva al ciberespacio. Las leyes parecen estar orientadas hacia ciertos estratos sociales, dando la impresión de que no se aplican universalmente, sino que se aplican principalmente a los menos poderosos y conocidos.

El delito informático, como se desarrolló con anterioridad, surge de las tecnologías modernas y afecta diversos aspectos de la vida diaria, sobre todo en empresas y organizaciones, las inviertan grandes cantidades de dinero para proteger su información. No obstante, no se pueden ignorar los vacíos legales que aparecen en estos casos, ya que pueden comprometer la integridad, la ética y los derechos de propiedad intelectual de individuos u organizaciones. Estos vacíos legales a menudo dan origen a los "paraísos digitales" o "cibernéticos", que son escenarios donde algunos individuos se benefician de la falta de regulaciones o leyes específicas sobre el cibercrimen.

Se ha demostrado que el 95% de los crímenes relacionados con el ciberespacio quedan impunes. Esta afirmación se basa en informes del Ministerio del Interior de dicha nación, que también destacan la ciberdelincuencia como un fenómeno significativo a nivel nacional y global. Este problema no solo representa un riesgo social y económico, sino que también afecta a una gran parte de la población, poniendo en peligro aspectos personales, financieros y, de manera crucial, la infraestructura esencial. Una vez más se demuestra que uno de los factores recurrentes en la investigación de estos delitos es la insuficiente seguridad en los datos cibernéticos, lo que aumenta el riesgo de que estos hechos ocurran. Esta situación ha captado

la atención a nivel global, generando preocupación entre gobiernos y mercados internacionales. La magnitud del problema ha llevado a estos actores a reconocer la importancia crítica de proteger la información informática y a implementar medidas de seguridad para mitigar el riesgo asociado.

El esfuerzo global para prevenir y sancionar la cibercriminalidad llevó a la creación de un convenio internacional sobre este tema, suscrito en Budapest, Hungría, en 2001, y ratificado por España el 1 de octubre de 2010. Este acuerdo subraya la necesidad de abordar delitos como el acceso no autorizado a sistemas informáticos, la interceptación de redes de comunicación, la creación y venta de herramientas para intrusión en sistemas, la alteración o eliminación de datos, fraudes en línea, espionaje cibernético y ataques a la propiedad intelectual y derechos relacionados (Acosta, Benavides y García, 2020).

En tal sentido, la impunidad en los delitos informáticos debe ser abordada desde perspectivas legales, axiológicas y de seguridad. Las organizaciones han enfrentado problemas relacionados con la seguridad de sus bases de datos, lo que las coloca en una posición vulnerable para proteger su información. Como se ha mencionado, esta vulnerabilidad contribuye al aumento de la cibercriminalidad, ya que los delincuentes aprovechan estas debilidades para perpetrar sus delitos. Enfatizar el cumplimiento de las normas y parámetros legales ayudará a proteger a quienes actualmente se encuentran desamparados frente a estas amenazas.

La seguridad cibernética es esencial para proteger y asegurar la información. Implementar políticas de protección de datos es un método clave para abordar esta problemática, junto con la adopción de programas internos de auditoría de sistemas que puedan alertar sobre cualquier irregularidad, como accesos no autorizados o violaciones de seguridad por parte de usuarios en la red.

En Perú, el enfoque principal es tanto la prevención como la sanción de las infracciones a la ley de seguridad cibernética. Es notable que el organismo encargado de hacer cumplir esta ley se apoya completamente en herramientas cibernéticas, aplicando recomendaciones para reducir riesgos y demostrando que la prevención y la seguridad son fundamentales. Por su parte, Costa Rica, al igual que Perú, centra su legislación en proteger la integridad y la confidencialidad de la información cibernética, enfocándose en sancionar a los infractores que atacan de manera desleal a los usuarios y sus datos.

2.1.3. Marco legislativo internacional

La figura de los delitos informáticos y la ciberdelincuencia en el marco internacional está principalmente defendida por el convenio de Budapest sobre la ciberdelincuencia el cual busca armonizar leyes nacionales y sobre todo mejorar la cooperación internacional estableciendo estándares para la investigación de los delitos informáticos.

a) Convenio de Budapest

En 2001 se adoptó el Convenio de Budapest, un avance normativo internacional sobre la ciberdelincuencia. Inicialmente dirigido a Estados miembros del Consejo de Europa, ha recibido adhesiones globales. El convenio establece estándares internacionales y definiciones comunes sobre criminalidad informática y sus modalidades. Regula la protección de evidencias digitales y criterios para la cooperación internacional. La ciberdelincuencia, por su naturaleza supranacional, requiere un compromiso duradero de los Estados para desarrollar políticas efectivas. Es crucial que las normativas de cada país sean coherentes y no contradictorias, orientadas a mitigar y sancionar conductas ilícitas, protegiendo los derechos de las personas más vulnerables ante estos delitos.

En ese sentido, el Convenio de Budapest es la norma internacional más completa para prevenir el riesgo a la confidencialidad, integridad y disponibilidad de sistemas y datos

informáticos. Se enfoca en tipificar delitos relacionados con el abuso de estos sistemas en las legislaciones nacionales, facilitando su detección y sanción mediante una cooperación internacional efectiva. El convenio abarca cuatro áreas principales de ciberdelitos:

- Delitos contra la confidencialidad e integridad de datos: acceso ilícito, interceptación ilícita, ataques a datos y sistemas.
- Delitos informáticos: falsificación y fraude informático.
- Delitos relacionados con contenido: pornografía infantil.
- Infracciones a la propiedad intelectual.

Además, promueve la responsabilidad penal de personas jurídicas por ciberdelitos cometidos por directivos o por falta de control. En el ámbito procesal, se impulsa la adopción de herramientas para la investigación de ciberdelitos, incluyendo la conservación y obtención de datos en tiempo real, garantizando la eficacia del proceso judicial.

Convenio de Budapest, es necesario reconocer el Convención de las Naciones Unidas contra la Ciberdelincuencia, debido que, en respuesta a la evolución de las tecnologías y los desafíos de la ciberdelincuencia, las Naciones Unidas han estado trabajando en un nuevo tratado internacional. En agosto de 2024, los Estados miembros de la ONU alcanzaron un acuerdo respecto de una nueva convención mundial contra la ciberdelincuencia, también conocida como la "Convención amplia contra el uso de las tecnologías de información y comunicaciones con fines delictivos".

De esa forma, este tratado busca establecer un marco jurídico global más amplio para prevenir y combatir los ciberdelitos, y establece estándares internacionales que ayudarán a proteger a los ciudadanos y a las economías de los Estados miembros. Su importancia radica en su alcance universal y en el hecho de que aborda la necesidad de una cooperación internacional más robusta en esta área. En esa misma línea, si bien se ha detallado dos

convenios importantes, siendo los instrumentos más influyentes a nivel global, existen otros instrumentos que contribuyen a la investigación de delitos informáticos, ya sea por su enfoque regional o por abordar aspectos específicos de la cooperación judicial:

El Protocolo adicional al Tratado sobre Ciberdelincuencia busca penalizar las acciones racistas y xenófobas cometidas mediante tecnologías informáticas. Además, un segundo Protocolo adicional tiene como objetivo solucionar la dificultad de obtener pruebas electrónicas en otros países.

b) Tratados de Asistencia Judicial Mutua

Del mismo modo, están los tratados de Asistencia Judicial Mutua**,** aunque no son específicos para delitos informáticos, los MLATs son fundamentales para la cooperación transfronteriza en la obtención de pruebas electrónicas. Muchos países tienen acuerdos bilaterales o multilaterales que permiten a las autoridades solicitar la asistencia de otro país para obtener información o pruebas relacionadas con una investigación criminal.

En ese sentido, como se evidencias, diversas regiones han desarrollado sus propios marcos, como la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales de 2014, que complementan los esfuerzos globales.

2.1.4. Legislación Comparada

En legislaciones comparadas podemos encontrar que otros países han implementado la figura del derecho informático en su ordenamiento jurídico, es por ello, que a modo de comparación desarrollaremos los países que han adoptado esta figura y la implementación de políticas públicas para el tratamiento de la ciberdelincuencia.

a) México. Se ha implementado una estrategia nacional de seguridad cibernética que propicia el uso responsable de las tecnologías de la información, contribuyendo al desarrollo sostenible. Cuenta con el CERT-MX, bajo la supervisión de la Policía

Federal, para enfrentar amenazas cibernéticas. Se han fomentado oportunidades de estudio en ciberseguridad y se han realizado foros específicos. Aunque no existe una ley dedicada al cibercrimen, el artículo 211 del Código Penal tipifica delitos informáticos, lo que presenta desafíos en la lucha contra el cibercrimen.

b) Costa Rica. Este país cuenta con el Ministerio de Ciencia, Tecnología y Telecomunicaciones (MICITT) desde 2017, que busca guiar el uso seguro de las tecnologías de la información. En 2012 se estableció un CSIRT para gestionar incidentes informáticos, colaborando con la red CSIRT Américas. Este equipo, formado por expertos en ciberseguridad, tiene como objetivo prevenir y responder a incidentes cibernéticos en instituciones gubernamentales y promueve políticas respaldadas por 69 miembros de entidades públicas y privadas.

c) Colombia. El país ha implementado un plan nacional para fortalecer las habilidades en seguridad digital, creando un Comité de Seguridad Digital liderado por el Coordinador Nacional de Seguridad Digital. El Ministerio de Tecnología y Comunicaciones (MinTIC) apoya la aplicación de medidas efectivas para proteger bienes de información esenciales. Además, bajo el Ministerio de Defensa, se gestionan incidentes cibernéticos y se resguarda la infraestructura crítica. Los ciudadanos tienen acceso a programas de pregrado y posgrado en ciberseguridad, y la nación mantiene vínculos con Interpol y Europol.

d) Chile. Este país desarrollo una estrategia nacional de seguridad cibernética a través de la Unidad de Coordinación de Ciberseguridad, que promueve diversas medidas, incluyendo el fortalecimiento del CSIRT de Gobierno, dependiente del Ministerio del Interior. Con el apoyo del Banco Interamericano de Desarrollo, se trabajan en evaluaciones y mejoras en la preparación y respuesta en ciberseguridad. Además, Chile participa en CSIRT Américas para facilitar el intercambio de información. La Alianza

Chilena de Ciberseguridad reúne a organizaciones del sector público y privado para fomentar la educación y comunicación.

***e) Estados Unidos*.** Estados Unidos aborda el desafío de la ciberseguridad mediante una combinación de regulaciones, políticas y el establecimiento de un Coordinador Nacional de Seguridad Cibernética. Este coordinador colabora con agencias gubernamentales y empresas privadas para coordinar una respuesta unificada a los incidentes en el ciberespacio. Además, el país cuenta con un Centro de Análisis e Intercambio de Información y la Comisión Federal de Comercio (FTC), que brinda orientación sobre la protección de datos. El Mes de la Concienciación sobre la Ciberseguridad Nacional, establecido en 2004, busca promover una cultura de seguridad en el uso de dispositivos conectados e incentivar carreras en ciberseguridad en instituciones tecnológicas. Las leyes también obligan a las entidades a informar sobre violaciones de seguridad de información personal.

El equipo ICS-CERT, que facilita servicios analíticos y asistencia, trabaja en alianza con empresas clave. El FBI, junto con la Agencia Nacional de Seguridad, lidera la investigación de delitos informáticos. La ciberseguridad se ha convertido en una prioridad de inversión para el gobierno y el sector privado en este país, reconocido por su avance tecnológico.

En ese sentido, y conforme a todo lo mencionado por los diversos países se puede evidenciar la presencia de la figura de los delitos informáticos y la ciberdelincuencia, sin embargo, también se puede afirmar la falta de políticas públicas eficiente que puedan facilitar la persecución eficaz de los delitos informáticos a fines de garantizar los derechos de las víctimas y evitar la impunidad del delito.

2.1.5. Sistema Acusatorio Penal

Nuestro sistema legal actual opera bajo un modelo acusatorio, caracterizado por una clara separación de funciones entre los participantes. Esto implica que las tareas de investigación y juicio son distintas, recayendo en el fiscal y el juez, respectivamente. El Ministerio Público es el responsable de perseguir los delitos públicos. Además, el sistema enfatiza los principios de oralidad y contradicción en las audiencias judiciales. También busca fortalecer las garantías legales tanto para el acusado como para la víctima, asegurando que ambos tengan igualdad de oportunidades para participar. Así, el autor Salinas (2020) explicó que, el modelo es acusatorio existe una separación de roles, el fiscal y el juez, el primero investiga y acusa, y el segundo juzga y resuelve. (p.56).

En ese sentido, se puede desprender que el sistema acusatorio es caracterizado por la separación de roles entre los distintos sujetos procesales, a fines de garantizar un proceso justo y equitativo.

2.1.5.1 Titularidad de la acción penal. Referirnos al titular de la acción penal en nuestro ordenamiento jurídico implica conocer el rol del Ministerio Público, que es responsable del ejercicio público de la acción penal y de la carga de la prueba. Desde la reforma procesal penal, este órgano jurisdiccional conduce la investigación y coordina tareas con la Policía Nacional, asumiendo un rol clave en el sistema judicial.

En ese sentido, el Ministerio Público es un organismo autónomo encargado de promover la acción penal en defensa de la legalidad y los intereses públicos. Posee autonomía funcional e imparcialidad, lo que asegura que su labor no sea interferida por otros poderes del Estado. Su actuación está regulada por el artículo 158° de la Constitución y por los artículos 60° al 66° del Código Procesal Penal, apoyándose en la Policía como órgano auxiliar según el artículo 67° del mismo código. Así, podemos afirmar que es el Estado el único que tiene la potestad soberana para perseguir delitos de ejercicio público y faltas.

2.1.5.2 Rol del Fiscal

Como se mencionó líneas arriba, el rol del fiscal es dirigir la investigación preparatoria y puede realizarlas por sí misma o encomendar a la policía las diligencias de investigación que estime direccionadas al esclarecimiento de los hechos (por iniciativa propia o solicitud de parte). Asimismo, es en el encargado de formular su acusación y promover la acción penal contra los autores y participes del proceso, que luego debe ser acreditado en la etapa de juzgamiento, según lo establecido por el art. 60.2 de NCPP.

2.1.5.3 Persecución eficaz del delito

Nuestro ordenamiento jurídico ha implementado reformas significativas en cuerpo normativo penal, cambiando del sistema inquisitivo al acusatorio. Aunque este nuevo sistema ha enfrentado modificaciones y ajustes, ha progresado en la eliminación de prácticas inquisitivas en la justicia. Históricamente, el país pasó del código de 1960 al de 1991, y finalmente al de 2004. Desde la perspectiva de eficiencia, el nuevo código ha demostrado ser efectivo al respetar los derechos fundamentales y la supremacía constitucional. Destacan organismos internacionales la importancia de que el proceso penal garantice una justicia accesible, rápida y coherente, involucrando no solo a especialistas en derecho, sino también a otras autoridades del sistema judicial.

Así, se aborda la persecución efectiva en el proceso penal, destacando la importancia del principio de legalidad y su relación con la eficacia del control social. Esta reforma introdujo el principio de oportunidad, que busca reemplazar un sistema inquisitivo obsoleto, generando un debate sobre su naturaleza. La legalidad asegura la aplicación de normativas, esencial para una tutela jurisdiccional efectiva en el debido proceso. Además, el objetivo del proceso penal no se limita a imponer penas, sino a resolver conflictos derivados de delitos de manera adecuada. La búsqueda de soluciones alternative está fundamentada en el garantismo, que

limita el poder del Estado en favor de los derechos fundamentales, como se refleja en la Constitución y los tratados internacionales.

Es evidente, que las reformas legislativas que ha tenido nuestro cuerpo normativo procesal buscan una persecución penal efectiva en vista a la evolución constante desde el sistema inquisitivo hacia un sistema mixto que, aunque teóricamente respetaba derechos, en la práctica se asemejaba al anterior.

El Código actual busca principalmente la eficiente persecución de delitos, comenzando con la información criminal que recibe el Ministerio Público. El fiscal realiza las investigaciones iniciales y luego se avanza a la fase preparatoria formal, donde se ejecutan actos de indagación en conjunto con la Policía. El Estado tiene la autoridad para ejercer la acción penal en todos los crímenes de interés público, con el Ministerio Público liderando la investigación y el juez administrando justicia. Según Flores (2016), la persecución penal es una obligación estatal que ostenta el control exclusivo de la acción penal, facultando a la Fiscalía para investigar, imputar cargos y defender en juicio hasta la sentencia, todo con el fin de identificar a los responsables de los delitos y sustentar la acusación con evidencias.

Cuando nos referimos a la persecución eficaz del delito hacemos referencia al proceso legal mediante el cual el titular de la acción penal, en este caso, el Ministerio público, acusa a los presuntos delincuentes con el objetivo de garantizar la aplicación de la justicia es importante mencionar que este proceso está basado en el principio de legalidad y su importancia se radica en lograr mantener el orden social en la sociedad.

Según Medina Valladares (2023) refiere que, la persecución del delito inicia con el pleno conocimiento de la noticia criminal por parte de la acción del titular penal, en ese caso el fiscal una vez que haya tenido conocimiento de dichos hechos procede a iniciar las diligencias preliminares para luego seguir con la etapa preparatoria formalizada.

Es importante resaltar que, en toda esta serie de investigaciones pueden ser apoyadas por parte de la policía a través de sus unidades especializadas en investigación criminal

2.1.6. Marco Conceptual

- **Ciberdelincuencia:** Según el Convenio Iberoamericano de Cooperación sobre Investigación, Aseguramiento y Obtención de Prueba en Materia de Ciberdelincuencia (2004), se considera ciberdelincuencia a cualquier tipo de delito cometido en el contexto de la interacción social que esté definido por el uso de las Tecnologías de la Información y la Comunicación (TIC).
- **Delitos informáticos:** Según Tejada (2017), se refiere a acciones ilegales llevadas a cabo mediante el uso indebido de la tecnología. Estas acciones ponen en peligro la privacidad de la información ajena al dañar o sustraer cualquier tipo de datos almacenados en dispositivos o servidores.
- **Derecho Penal:** Rama legal encargada de normar conductas directivas y establecer las acciones correspondientes a aquellos que las infringen (Andrade, 2021).
- **Diligencias Preliminares:** Según Barrios (2017), se entiende por estas las intervenciones iniciales que realiza la Policía Nacional o el Ministerio Público, inmediatamente después de conocer la posible comisión de un acto con características de delito.
- **Fiscal:** Es el titular y director de la investigación cuya obligación está al frente de la mayor cantidad de diligencias preliminares que disponga a realizar en su caso para el esclarecimiento de los hechos (Salinas, 2015).
- **Ministerio Público:** Es la persona responsable de la investigación preliminar y de llevar a cabo la acción penal, quien previene y persigue el delito, defiende la ley, y además protege a las víctimas y testigos de un crimen (García, 2018).
- **Seguridad jurídica:** Según Chavarría (2023), este es un principio del derecho aceptado globalmente, basado en la claridad de la ley tanto en su difusión como en su aplicación.

Implica la certeza de que se conoce, o se puede conocer, lo que está prohibido, mandado o permitido por la autoridad pública.

- **Tecnologías de la información:** De acuerdo con Gil (2002), las TIC se describen como el total de sistemas, técnicas, herramientas, métodos y aplicaciones cuyo objetivo es convertir textos, sonidos, imágenes y señales analógicas en formatos digitales que pueden ser administrados en tiempo real.

III. MÉTODO

3.1. Tipo de Investigación

La actual investigación, es de tipo básico, la cual tuvo como finalidad generar conocimiento científico orientado a identificar las causas que limitan una persecución eficaz del delito informático en las fiscalías especializadas en ciberdelincuencia. Como señala Hernández, Fernández y Baptista (2014), la investigación básica se enfoca en la comprensión profunda de fenómenos, sin perseguir necesariamente una aplicación inmediata, lo cual resulta pertinente en el estudio del fenómeno delictivo digital, cuyas dinámicas evolucionan constantemente.

Aunado a ello, Según Zabalza (1988), señala que el enfoque cualitativo se caracteriza por la recolección de información a través de la observación directa y diversos métodos de evaluación. A partir de los vínculos identificados en los datos, se construyen categorías y se formulan teorías emergentes. El objetivo principal consiste en desarrollar una teoría que respalde los hallazgos obtenidos. Esta construcción teórica se logra mediante el análisis comparativo de fenómenos semejantes y distintos, lo que permite elaborar una explicación coherente de la realidad estudiada.

3.1.1. Nivel de investigación

Esta investigación es de tipo descriptivo y explicativo. Por un lado, busca caracterizar el fenómeno de los delitos cibernéticos en el sistema de justicia penal. Por otro, intenta identificar y examinar las razones que limitan la efectividad de las Fiscalías Especializadas en Ciberdelincuencia. En su faceta descriptiva, el estudio pretende ofrecer una visión clara de la ocurrencia de delitos informáticos en Perú, con énfasis en Lima Metropolitana. Para ello, se detallará el funcionamiento de estas fiscalías especializadas, sus procedimientos de

investigación y los tipos de ciberdelitos más frecuentes. Finalmente, el enfoque explicativo va más allá de la descripción, concentrándose en comprender las causas profundas que impactan la eficacia de la persecución penal de los delitos informáticos.

3.1.2. Diseño de investigación

Esta investigación emplea un diseño no experimental, pues su objetivo principal es analizar la relación entre dos elementos clave: primero, los factores institucionales, normativos y operativos que inciden en el desempeño de las Fiscalías Especializadas en Ciberdelincuencia; y segundo, la efectividad de la acción penal frente a los delitos cibernéticos en Lima Metropolitana.

En línea con esto, Hernández, Fernández y Baptista (2014) señalan que un diseño no experimental es aquel donde las variables no se manipulan intencionalmente, sino que los fenómenos se estudian tal como ocurren en su entorno natural. En este sentido, el investigador no interviene en el desarrollo de los hechos, sino que recoge y analiza la información existente a partir de su manifestación en la realidad, lo que resulta especialmente adecuado para estudios en los que no es posible, viable o ético alterar las condiciones del entorno.

3.2. Ámbito temporal y espacial

La investigación ha sido delimitada geográfica y temporalmente de la siguiente manera:

- **Ámbito espacial**

El ámbito espacial del estudio está delimitado al departamento de Lima, con especial énfasis en las Fiscalías Especializadas en Ciberdelincuencia ubicadas en Lima Centro, las cuales constituyen el eje principal del análisis por su competencia directa en la investigación y persecución de delitos informáticos. Al centrar la investigación en esta área geográfica, se

busca obtener una comprensión más profunda y contextualizada de los factores que limitan la eficacia de dichas fiscalías frente al fenómeno creciente de la criminalidad digital, permitiendo identificar con mayor precisión las deficiencias estructurales, normativas y operativas que afectan su desempeño.

- **Ámbito temporal**

En cuanto al ámbito temporal, el estudio se circunscribe al año 2024, periodo durante el cual se recopilaron los datos relevantes y se llevaron a cabo las entrevistas con operadores del sistema de justicia penal vinculados a la investigación y procesamiento de delitos informáticos. Este marco temporal permite analizar con mayor precisión las condiciones actuales en las que operan las Fiscalías Especializadas en Ciberdelincuencia, así como las limitaciones técnicas, normativas y organizacionales que inciden en su eficacia frente a la creciente complejidad de los delitos cibernéticos en el contexto nacional.

3.3. Variables

Una variable de investigación se define como un concepto que permite hablar sobre la conexión entre causa y efecto. Así, representa un atributo que se puede medir y cuyos resultados cambian al utilizar diferentes herramientas.

Tabla 1

Matriz de categorización

CATEGORÍAS	SUBCATEGORÍAS
EFICACIA DE LA INVESTIGACIÓN FISCAL	● Causas de la ineficiencia de la investigación fiscal. ● Consecuencias de la ineficiencia de la investigación fiscal.

	● Medidas correctivas para mejorar la investigación fiscal del delito.
DELITOS INFORMÁTICOS	● Diligencias preliminares en delitos informáticos ● Actividades probatorias ● Identificación del sujeto activo.

Fuente: Elaboración propia

3.4. Población y muestra

3.4.1. Población

La población de la presente investigación está compuesta por los operadores del sistema de justicia penal que intervienen directa o indirectamente en la persecución de los delitos informáticos en la ciudad de Lima. Especialmente, la población está compuesta por la población a los jueces penales, fiscales especializados en ciberdelincuencia y abogados penalistas que desempeñan funciones en instituciones relacionadas con la investigación, juzgamiento y defensa en casos vinculados al cibercrimen.

De esa forma, estos actores jurídicos fueron seleccionados por su rol clave en el desarrollo de procesos penales en referencia con delitos informáticos, y por ser quienes enfrentan, desde diferentes perspectivas, las limitaciones normativas, técnicas y operativas que obstaculizan una respuesta eficaz frente a esta modalidad delictiva. En especial, se presta atención a los fiscales pertenecientes a las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro, por su competencia directa en la investigación de este tipo de ilícitos.

3.4.2. Muestra

La selección de la muestra no es aleatoria, y se utiliza un método deliberado. Los requisitos para participar son que los operadores jurídicos deben ser expertos en el área penal.

- 3 jueces penales de la Corte Superior de Justicia de Lima
- 3 fiscales del Distrito Fiscal de Lima
- 6 abogados

Tabla 2

Lista de participantes

N°	Participantes	Nombre Completo	Cargo	Institución
1	Fiscal 1	Paola Vanesa Chajara Coata	Fiscal Provincial	Primera Fiscalía Corporativa Especializada
2	Fiscal 2	Elsa Lisbeth Sánchez Gutiérrez	Fiscal Adjunta Provincial	Primera Fiscalía Corporativa Especializada
3	Fiscal 3	P. María Sánchez Loayza	Fiscal Adjunto Provincial	Fiscalía Cibernética Lima Centro
4	Fiscal 4	Ángel Gonzales Farfán	Fiscal Provincial	Primer Despacho de la Fiscalía Corporativa Especializada
5	Fiscal 5	Yanina Imelda Orozco Huayanay	Fiscal Provincial	4to Despacho provincial de la segunda fiscalía Corporativa
6	Fiscal 6	Lery Rojas Huaino	Fiscal Adjunto Provincial	Primera Fiscalía Corporativa Especializada
7	Fiscal 7	Malena Ayala Gonzales	Fiscal Adjunta Provincial	Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro

3.5. Instrumentos de recolección de datos

La presente investigación utiliza tres instrumentos fundamentales para la recolección de datos. De esa forma, se recurre a la observación, la cual permitirá identificar de manera directa las características y dinámicas del fenómeno objeto de estudio en su contexto natural,

específicamente en lo relacionado con la actuación de las Fiscalías Especializadas en Ciberdelincuencia.

En segundo lugar, se aplica una guía de análisis documental, enfocada en el examen sistemático de resoluciones judiciales pertinentes. Este instrumento permitirá evaluar cómo se vienen resolviendo los casos vinculados a delitos informáticos, identificando patrones, criterios jurídicos aplicados y posibles limitaciones en la persecución penal.

Finalmente, se utilizará una guía de entrevista semiestructurada, dirigida a operadores jurídicos entre ellos jueces, fiscales y abogados penalistas con la finalidad de recoger información cualitativa sobre su percepción, experiencia y valoración respecto a los factores que afectan la eficacia en la investigación y sanción de los delitos cibernéticos. Estos instrumentos en conjunto permitirán obtener una visión integral y fundamentada del problema planteado.

3.6. Procedimientos

La presente investigación se ha desarrollado a través de la aplicación de una guía de análisis documental, centrada en el estudio de fuentes jurídicas relevantes, tales como jurisprudencia, doctrina y normativa vigente en materia de delitos informáticos. Para la implementación de este instrumento, se han seguido los siguientes procedimientos metodológicos:

En primera línea, se ha optado por la recolección y búsqueda de datos, cuya fase consistió en la identificación y recopilación de información directamente relacionada con la problemática de investigación. Es así como, en esta etapa inicial, se procedió a la búsqueda sistemática de material bibliográfico y documental, utilizando diversos recursos digitales. Por ello, se recurrió a repositorios académicos nacionales e internacionales, bases de datos jurídicas, revistas indexadas especializadas en derecho penal y tecnología, así como a

jurisprudencia sistematizada del Tribunal Constitucional y del Poder Judicial, con el fin de obtener fallos relevantes y actuales vinculados al delito informático.

Por otro lado, se optó por el análisis e interpretación de la información, siendo así que, en esta etapa, se aplicó la guía de análisis documental para examinar el contenido de las fuentes seleccionadas. El objetivo fue identificar elementos comunes, contradicciones y vacíos normativos o jurisprudenciales que incidan en la efectividad de las fiscalías especializadas en ciberdelincuencia.

Finalmente, los datos extraídos fueron sintetizados e integrados dentro del marco teórico de la investigación, permitiendo formular conclusiones coherentes y recomendaciones pertinentes en relación con el problema investigado.

3.7. Análisis de datos

La investigación emplea un método cualitativo centrado en el análisis documental, examinando a través de teorías y leyes. Este enfoque permite explorar las diversas interpretaciones teóricas y diferentes perspectivas académicas, lo que facilita una comprensión más profunda de los crímenes cibernéticos e identifica las dificultades prácticas que impactan la investigación fiscal.

3.8. Consideraciones éticas

La presente investigación ha sido desarrollada con estricto respeto a los principios éticos que rigen la labor científica. En esa línea, asumí el compromiso de aplicar medidas específicas que aseguren la integridad ética de esta tesis. En primer lugar, se garantizó la trasparencia de los datos brindados por los entrevistados, quienes participaron de forma voluntaria y con pleno conocimiento de los objetivos del estudio.

Asimismo, antes de cada entrevista, solicité el consentimiento informado de los participantes, los cuales se evidencia en los anexos de cada entrevista, explicándoles

claramente el propósito de la investigación. Esta práctica me permitió mantener un vínculo transparente y ético con cada uno de los profesionales consultados.

Por otro lado, mantuve el rigor académico en el tratamiento de fuentes jurídicas, doctrinarias y jurisprudenciales, garantizando la veracidad, precisión y adecuada citación de todo el contenido consultado. Me aseguré de no incurrir en plagio, falsificación de datos ni omisión de referencias, siendo así que cada idea o aporte ajeno fue correctamente atribuido, respetando los derechos de autor y aplicando criterios éticos en el uso de la información documental.

IV. RESULTADOS

En el presente capitulo son exhibidos todos aquellos resultados que fueron obtenidos, tras la aplicación de la guía de entrevista con la que fueron recogidas las diferentes opiniones que emitieron los especialistas en derecho penal, tal como a continuación se describe:

El **objetivo general** es, determinar cómo influye la investigación fiscal en la eficacia de la sanción de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024:

La **primera pregunta**: ¿Cuál es el impacto del delito informático en nuestra ciudad?

Tabla 3

Resultados de primera pregunta

Entrevistado	Opiniones emitidas
Fiscal 1	Impacta en diferentes áreas, en la confianza del sistema financiero a nivel del patrimonio de los ciudadanos y la seguridad digital y otros.
Fiscal 2	El delito informático ha ido en aumento junto con el avance de la tecnología, lo cual ocasiona nuevas modalidades de incurrir en ellos y estando a su realización por medios digitales es más complejo su persecución.
Fiscal 3	A raíz del COVID 19, donde la virtualidad estuvo en todo su auge se pudo advertir el incremento de estos delitos informáticos, el cual se ha visto perfeccionado, dado que son delitos donde prima el anonimato.
Fiscal 4	Negativo y múltiple pues puede considerárseles como pluriofensivo, al comprometer varios bienes jurídicos protegidos: patrimonio, identidad, intimidad, seguridad, indemnidad sexual, etc.

Fiscal 5	Positivo y Negativo, ya que al obtener el avance tecnológico se puede garantizar optimo avance para la seguridad informática; negativo debido que no todos manejan con responsabilidad el uso de las TIC.
Fiscal 6	Por el incremento del avance tecnológico los delitos informáticos se han visto incrementados de manera acelerada.
Fiscal 7	El impacto que ha traído consigo los delitos de informáticos – previsto en la Ley 30096 y sus modificaciones- es frenar el gran avance que se ha venido dando sobre la comisión de delitos bajo esta modalidad, busca hacer una lucha frontal y tener los mecanismos para no dejar impune esta nueva forma de delinquir, pues de no contar con tal normativa muchos actos que han generado gran perjuicio a las víctimas habrían quedado impunes.

Fuente: Elaboración propia

Interpretación analítica:

Los entrevistados concuerdan en que los delitos informáticos constituyen una amenaza creciente, potenciada por el avance acelerado de la tecnología y el auge de la virtualidad, especialmente tras la pandemia por COVID-19. Coinciden en que estos ilícitos comprometen diversos bienes jurídicos, desde el patrimonio y la identidad hasta la seguridad digital y la intimidad, lo que demuestra su carácter pluriofensivo. Además, señalan que su persecución resulta compleja debido al anonimato y a las constantes innovaciones tecnológicas. En cuanto a las diferencias, algunos enfatizan el impacto negativo de estos delitos sobre la confianza ciudadana en el sistema financiero, mientras que otros reconocen tanto aspectos positivos como negativos, resaltando que el desarrollo tecnológico también puede fortalecer la seguridad informática si se gestiona adecuadamente. Finalmente, se valora la existencia de un marco

normativo específico como la Ley 30096, que permite enfrentar de manera más eficaz esta modalidad delictiva y evitar la impunidad.

Siguiendo esa línea, el **primer objetivo específico,** es determinar cuáles son las causas que limitan realizar una persecución eficaz de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

Segunda pregunta: De acuerdo con su experiencia ¿Considera que la conducta de la víctima contribuye a la perpetración del delito informático?

Tabla 4

Resultados de segunda pregunta

Entrevistado	Opiniones emitidas
Fiscal 1	Sí, ya que en muchos delitos informáticos es necesario para su perpetración el error humano, donde los ciberdelincuentes aprovechas dicho error para ingresar obtener sus claves o irrumpir en su entorno digital.
Fiscal 2	Depende de la modalidad del delito, existen algunas modalidades como el phishing o el vishing que son bastantes conocidos y difundidos por medios periodísticos con la finalidad de prevenirlos, sin embargo, pese a ello, la población no se informa e incurre de forma reiterada en estas modalidades delictivas. Por otro lado, existen otros delitos que requieren un acceso ilícito a sistemas, para su comisión y por más cuidados que la víctima pueda tener, se está expuesta a ellos.
Fiscal 3	Claro que sí, ya que el desconocimiento de los agraviados en no brindar sus confidenciales bancarios y a ingresar a enlaces falsos- fishing, es el común de los delincuentes para cometer delitos ilícitos.
Fiscal 4	No por su conducta, aunque sí pro su “condición”, debido a la brecha digital, no todos son conscientes de la importancia de la ciberseguridad al momento de utilizar las tecnologías de la información y la comunicación (TIC).
Fiscal 5	Sí, porque con el avance de la tecnología la población no se encuentra informada que, ante cualquier error en la introducción de sus datos personales

	o el contenido de sus tarjetas, los ciberdelincuentes aprovechan generándoles un perjuicio económico.
Fiscal 6	La falta de conocimiento en temas informáticos y la poca difusión de medidas preventivas genera vulnerabilidad en las victimas.
Fiscal 7	No, debido a que existen múltiples modalidades que se vienen conociendo al hacer las investigaciones se aprecia que existe un déficit de seguridad en entidades bancarias y en algunas empresas, al haber una falta de implementación de programas que ciberseguridad, lo que termina poniendo en una situación de riesgo a la víctima (persona natural o jurídica); no obstante, si bien existe un porcentaje donde las víctimas de alguna manera facilitan algunos datos que contribuyen a la comisión de los delitos, este aspecto no puede ser atribuible a la misma pues ante la globalización que se viene afrontando no se puede exigir que las personas conozcan o tenga acceso a información respecto de la tecnología.

Fuente: Elaboración propia

Interpretación analítica:

Los entrevistados concuerdan en que, en muchos casos, la víctima puede desempeñar un rol indirecto en la comisión de delitos informáticos, ya sea por desconocimiento, descuido o falta de cultura digital. Coinciden en que el error humano, como compartir información confidencial o acceder a enlaces fraudulentos, es un factor que los ciberdelincuentes suelen aprovechar. Sin embargo, difieren en cuanto al grado de responsabilidad atribuible a las víctimas. Algunos sostienen que la conducta de la persona facilita el delito, mientras que otros matizan esta idea, argumentando que la vulnerabilidad se debe más a una falta estructural de educación digital, desigualdades tecnológicas y deficiencias en la seguridad institucional. También se destaca que, aunque existen campañas de prevención, no siempre son suficientes o efectivas. En suma, mientras unos señalan la corresponsabilidad de las víctimas, otros enfatizan que no puede exigirse a todos el mismo nivel de conocimiento tecnológico en un contexto de brecha digital.

La **tercera pregunta**: De acuerdo con su experiencia ¿Considera que la conducta de las entidades financieras en caso de fraude tarjetas de crédito contribuye a la perpetración del delito informático?

Tabla 5

Resultados de tercera pregunta

Entrevistado	Opiniones emitidas
Fiscal 1	Sí, en algunos casos las medidas de validación no son lo suficientemente seguras, lo que facilita suplantaciones de identidad, en otros casos el personal contratado por el banco no es idóneo y cometen fraudes u otros delitos.
Fiscal 2	En cierta medida, debido a que no implementan mecanismos de seguridad relacionadas al uso de las tarjetas en comercios, como por ejemplo contar con un CVV virtual y no físico.
Fiscal 3	Creo que el banco no contribuye a la perpetración del delito, ya que son los usuarios los responsables del uso tarjetas, pero si considero que su rechazo de los bancos y la mala información contribuyen a la no identificación de los investigados.
Fiscal 4	Si se verifica o demuestra que, una entidad “omite” velar por el incremento de sus niveles de ciberseguridad, quizás sí podría informar que esa omisión contribuye a la perpetración del delito.
Fiscal 5	Si, porque muchas veces sus medidas de seguridad son vulneradas, al no obtener un manejo responsable como entidad financiera, y el uso poco responsable de sus usuarios.
Fiscal 6	Si, la falta de sistemas y mecanismos justificados contribuye a la comisión de delitos informáticos, aunado a la poca difusión preventiva de las entidades.

Fiscal 7	Si, lamentablemente sus políticas de prevención de fraude que viene ostentando no son seguras ni resultan eficaz para combatir o frenar los casos de fraude con tarjetas de crédito, pues resulta muy fácil realizar operaciones con tan solo conocer las credenciales de acceso de las tarjetas de créditos, pese a que es de conocimiento público que en la actualidad existe un mercado negro donde se puede conseguir tal información. Por lo que, es de imperiosa necesidad que tales entidades mejoren sus políticas e implementen mayores planes de ciberseguridad.

Fuente: Elaboración propia

Interpretación analítica:

Los entrevistados concuerdan en que las entidades bancarias, en diversos grados, contribuyen a la comisión de delitos informáticos, principalmente debido a la debilidad de sus sistemas de seguridad y la falta de políticas eficaces de prevención del fraude. Existe consenso en que las medidas adoptadas por los bancos son, en muchos casos, insuficientes para evitar suplantaciones de identidad, fraudes con tarjetas y filtración de datos sensibles.

Asimismo, se señala que la omisión de reforzar los niveles de ciberseguridad o de implementar mecanismos modernos, como el CVV virtual, expone a los usuarios a mayores riesgos. Sin embargo, algunos entrevistados puntualizan que, si bien existen deficiencias institucionales, los usuarios también tienen responsabilidad en el uso correcto de sus datos. A pesar de esta diferencia, todos coinciden en que urge una mejora sustancial en las políticas de seguridad de las entidades bancarias para prevenir eficazmente estos delitos.

Siguiendo esa línea, el **segundo objetivo específico,** es determinar las cuáles son las consecuencias que conlleva la falta de identificación de los partícipes del delito informático

para garantizar una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

Ante ello, se formularon las siguientes interrogantes:

La **cuarta pregunta**: De acuerdo con su experiencia ¿Cuáles son las implicancias que conlleva falta de identificación de los partícipes del delito informático?

Tabla 6

Resultados de cuarta pregunta

Entrevistado	Opiniones emitidas
Fiscal 1	Conlleva al archivo de las denuncias o la impunidad de algunos de los implicados del hecho.
Fiscal 2	La principal es la impunidad, debido a que no se logra una sanción penal para ello, así como tampoco prevenir su participación en hechos similares, y, por otro lado, el hecho de que el agraviado no conozca quien se apoderó de su dinero y no vea satisfecho el perjuicio ocasionado.
Fiscal 3	1.- Que los policías no solicitan información de cámaras o no la recaban cuando se pone denuncia. 2.- Que el banco demora en remitir respuesta y no resguardan cámaras. 3.- Que el banco no informa los datos de los comercios donde realizaron operaciones no reconocidas.
Fiscal 4	La propia naturaleza del entorno digital de los delitos informáticos, que lo convierten en delitos con entornos furtivos o clandestinos.
Fiscal 5	Archivos de denuncias, impunidad para algunos responsables del hecho, el banco no remite información detallada que permita coadyuvar al esclarecimiento del hecho.

Fiscal 6	La falta de mecanismos informáticos por parte de las entidades encargadas en la persecución de dichos delitos genera impunidad e impide sanciones a los avances directos de delitos informáticos.
Fiscal 7	Debo comenzar indicando que al ser delitos informáticos una de las características de la misma es que el sujeto activo no es fácil de identificar, por tal motivo de no poder identificarse autores o coautores lamentablemente la investigación no será fructífera y deberá ser archivada pues conformé lo prevé el artículo 336 del CPP se debe " individualizar al sujeto activo"; sin embargo, cabe precisar que si se logra identificar al cómplice primario y/o secundario pero no al autor o coautor, pero si se puede verificar la existencia del mismo dentro de los hechos, si resulta viable proseguir la causa.

Fuente: Elaboración propia

Interpretación analítica:

Los entrevistados concuerdan en que las dificultades para identificar a los autores de los delitos informáticos generan altos niveles de impunidad y el consecuente archivo de las denuncias, lo que impide sancionar a los responsables y resarcir adecuadamente a las víctimas. Coinciden en que esta problemática se ve agravada por la naturaleza clandestina del entorno digital, la falta de colaboración oportuna de las entidades bancarias, la omisión de diligencias policiales (como la solicitud de cámaras) y la carencia de mecanismos informáticos adecuados en las instituciones encargadas de la persecución penal. Aunque todos reconocen la complejidad de la individualización del sujeto activo, algunos matizan que, si bien es difícil identificar al autor directo, la investigación podría continuar si se logra verificar la existencia

de cómplices o elementos objetivos del delito. En suma, la falta de eficiencia en la obtención de pruebas y la débil cooperación interinstitucional perpetúan la impunidad.

Del mismo modo, en referencia al **tercer objetivo específico,** es determinar cuáles serían las medidas correctivas que deberían adoptarse para realizar una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

A partir de la pregunta planteada, se formularon las siguientes interrogantes:

La **quinta pregunta**: En su opinión ¿Cuáles las medidas correctivas que deben adoptarse para hacer una persecución eficaz al delito informático?

Tabla 7

Resultados de quinta pregunta

Entrevistado	Opiniones emitidas
Fiscal 1	1. La especialidad es indispensable, es decir la capacitación especializada del investigador. 2. El apoyo adecuado por parte de las instituciones financieras y telecomunicaciones para brindar la información requerida. 3. La preservación de la evidencia digital y otros.
Fiscal 2	1.-Garantizar que la información no sea tan volátil y que pese el tiempo transcurrido aun pueda obtenerse (IPS, información bancaria, cámaras de seguridad, información comercial) copias espejo de dispositivos afectados, etc. 2.- Implementar mesas de trabajo tanto con las empresas operadoras bancarias y demás que participan en brindar información con la finalidad de garantizar una respuesta optima, rápida y de acuerdo con lo solicitado. 3. Implementar bases de datos que permitan compartir

	información a nivel fiscal sobre nombres de cuentas receptoras y demás partícipes en estos hechos delictivos.
Fiscal 3	1.-El banco asuma la deuda cuando no valida los datos correctamente, por parte de la SBS, que reciba sanción frente al incumplimiento. 2.- Que sanciones a las empresas telefónicas por no tener filtros correspondientes para evitar suplantación de identidad, por parte de OSIPTEL reciba sanción frente al incumplimiento.
Fiscal 4	Acceder a la información administrada por el sector privado (bancario /comunicaciones) en tiempo casi real.
Fiscal 5	Capacitaciones especializadas en ciberseguridad, el apoyo eficaz del sector privado y público para obtener información en tiempo y espacio real.
Fiscal 6	Adopción de mecanismos de lucha y sobre todo prevención en el ámbito de la informática
Fiscal 7	El Estado debe exigir que las políticas de ciberseguridad de las entidades bancarias sean mejoradas, de igual forma respecto de los sistemas de las entidades públicos debe procurar que exista mejores niveles de control y seguridad – invertir también en planes se seguridad cibernética - para evitar que se realicen ataques a los mismos, como se ha venido dado últimamente; y ante el avance de nuevas modalidades de la comisión del delito informático haciendo uso de criptomonedas urge la creación de una billetera estatal para poder lograr la incautación de las mismas.

Fuente: Elaboración propia

Interpretación analítica:

Los entrevistados concuerdan en que para fortalecer la lucha contra los delitos informáticos es fundamental mejorar la coordinación interinstitucional, contar con personal especializado y asegurar el acceso oportuno a la información digital relevante. Coinciden en la necesidad de capacitaciones en ciberseguridad para los operadores del sistema de justicia, así como en la importancia de que las entidades privadas especialmente bancos y operadoras de telecomunicaciones colaboren eficazmente en la entrega de datos y preservación de evidencias.

Asimismo, se propone que las instituciones reguladoras, como la SBS y OSIPTEL, apliquen sanciones frente al incumplimiento de protocolos de seguridad. Si bien algunos enfatizan la prevención mediante políticas públicas robustas y mecanismos de respuesta rápida, otros sugieren medidas específicas como bases de datos fiscales compartidas, creación de billeteras digitales estatales y sanciones a las entidades negligentes. En conjunto, se destaca la necesidad de una respuesta integral, técnica y normativa frente al avance de nuevas formas de criminalidad digital.

V. DISCUSIÓN DE RESULTADOS

Con base en lo que se logró observar a partir de los resultados del capítulo previo, respecto al **objetivo general**, de determinar cómo influye la investigación fiscal en la eficacia de la sanción de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

Hernández, (2009) señala que el delito informático representa una amenaza creciente impulsada por el avance tecnológico y que su impacto se extiende a múltiples ámbitos, como la seguridad, el patrimonio y la intimidad de las personas. Asimismo señala que la conducta de la víctima influye en ciertos delitos informáticos, especialmente cuando hay desconocimiento o errores humanos, así como factores estructurales como la brecha digital y la deficiente ciberseguridad institucional, eximiendo a la víctima de culpa directa; a su vez las entidades financieras, en gran medida, contribuyen a la perpetración del delito informático relacionado con fraudes en tarjetas de crédito, debido a la deficiencia en sus mecanismos de seguridad y políticas preventivas.

Por otro lado, los resultados armonizan con lo señalado por Martínez (2021), quien señala la necesidad de que se brinde una capacitación de los fiscales en Guerrero - México, para que ellos puedan actuar competentemente frente a estas denuncias de ciberdelitos. Asimismo, argumenta que los Ministerios Públicos no tienen una capacitación adecuada; limitando las perspectivas de estos, en comprender la conducta punible y sus afectaciones; no pudiendo hacer una acusación correcta; ocasionando que se produzca la impunidad en las carpetas de investigación, por la ausencia de pruebas.

Aunado a ello, Sánchez, (2019) señala que se deben instaurar policías que sean especializados sobre todo en ciberdelitos, para que, estos se puedan combatir, de esa forma el autor hace énfasis que en el Perú se debe dar una mayor descentralización de policías y también

de fiscales que se encuentren totalmente capacitados en estos temas de ciberdelitos; además de que se creen instituciones idóneas; y que haya una existencia recíproca por ambos países para combatir estos delitos.

Finalmente, Ayma, (2020), menciona que los ciberdelitos tienen relación con el mismo tiempo en que se ha elaborado la investigación preliminar; así indica que los procesos que están vinculados a estos delitos informáticos resultan ser ineficientes; causando desconciertos, como resultado de no darle un correcto tratamiento a la Ley de forma adecuada. También, al igual que los autores señalados anteriormente, pone en relevancia que las capacitaciones hacia el Ministerio Público deben darse de forma constante ya que son de vital importancia, para que de esta forma se realice una correcta investigación preliminar, sobre todo para los fiscales que llevan a cabo la investigación de los ciberdelitos.

Del **primer objetivo específico,** es determinar cuáles son las causas que limitan realizar una persecución eficaz de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

De esa forma, podemos señalar lo dicho por Shirakian (2021), quien señala que no existen medidas legislativas que sean fijadas para estos delitos informáticos, causando perjuicio y vulnerando de esta manera las garantías procesales además de los derechos de las partes que intervienen en el proceso, es por esa razón que se deben de incluir las medidas probatorias de acuerdo al principio de libertad probatoria, empero, este principio al aplicarse repetitivamente origina un perjuicio, contraviniendo de esta manera el principio de legalidad.

Asimismo, Hernández y Patricio (2020), a comparación del autor señalado líneas arriba, menciona el actuar de los fiscales, muchas veces afecta que se obtengan las pruebas, con más razón cuando no se tiene equipos ni softwares correctos, además influye la falta de fiscales especializados en este delito, también la poquísima colaboración de la policía y la

ineficiencia en la cooperación de las empresas que proveen la información; hacen que no se puedan tener pruebas efectivas y reales. El que no existan equipos y herramientas informáticas, es una realidad actual, la policía no coopera y las empresas proveedoras de servicios tampoco; no se evidencia claridad en los procedimientos, para poder obtener las pruebas; generándose un perjuicio a la investigación.

Por otro lado, Usaqui, (2022) menciona que estas actividades en el que se indaga preliminarmente logran repercutir la lucha en la realidad frente a los delitos informáticos. De tal modo, que a partir de las indagaciones que se realizan de forma previa; son porque no se tiene capacitaciones constantes; haciéndose de esta forma difícil en la obtención de pruebas; asimismo, para que se pueda localizar al ciberdelincuente, tiene que presentarse solicitud a las empresas que proveen servicios, sin embargo no se realiza ello, debido a que es necesario un fallo judicial, originando una demora para las pruebas; por último, estas insuficiencias para encontrar la información y su impedimento para poder reconocer al ciberdelincuente, son una de las causas principales para que no se puedan obtener las pruebas verídicas.

Se puede evidenciar a partir del análisis y los comentarios realizados por Usaqui (2022), la lucha contra los delitos informáticos enfrenta serias limitaciones en la práctica debido a la falta de preparación técnica y jurídica de los operadores encargados de la investigación. Este panorama deja entrever que, si bien existen marcos normativos que penalizan estas conductas, en la realidad, la ejecución efectiva de las investigaciones se ve obstaculizada por la escasa capacitación y la limitada articulación con entidades proveedoras de servicios digitales.

Un aspecto especialmente crítico es la dificultad para obtener pruebas digitales en tiempo oportuno. La necesidad de una orden judicial para solicitar información a empresas proveedoras de servicios tecnológicos genera una demora considerable, lo cual perjudica directamente la trazabilidad de los delitos cometidos en entornos virtuales. Asimismo, la

carencia de mecanismos ágiles para el reconocimiento e identificación de los ciberdelincuentes constituye una de las principales barreras para la judicialización efectiva de estos casos.

En este sentido, se vuelve evidente la urgencia de fortalecer las capacidades institucionales a través de programas de formación especializada en cibercriminalidad, así como la necesidad de establecer protocolos claros y cooperativos con las empresas tecnológicas. Solo así será posible garantizar una respuesta eficiente, respetuosa del debido proceso y centrada en la protección de los derechos de las víctimas.

Sobre el **segundo objetivo específico,** es determinar cuáles son las consecuencias que conlleva la falta de identificación de los partícipes del delito informático para garantizar una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024**.**

Del análisis documental se deduce, como señala Sotomayor (2022), que las evaluaciones fiscales en las investigaciones de delitos en línea no son efectivas para demostrar la existencia de dichos delitos, debido a los criterios establecidos en la evaluación fiscal; se encuentran conforme la norma procesal, observándose que estas investigaciones, son realizadas por lo general por la policía especializada en estos delitos informáticos, generando un error en la investigación; conforme a la Ley 30096, la cual señala que tiene un gran significado y un mayor progreso frente a las investigaciones, con las fiscalías que ya se encuentran establecidas, y que están dedicadas especialmente a estos delitos informáticos, para finalmente tener las pruebas convincentes.

Sin embargo, no es el único autor que hace énfasis en las calificaciones fiscales, debido a que Usaqui, (2022) señala que las actividades de investigación en el que se indaga preliminarmente logran repercutir la lucha en la realidad frente a los delitos informáticos.

Como se ha evidenciado en los resultados obtenidos, uno de los principales obstáculos en la lucha contra los delitos informáticos es la dificultad para localizar e identificar al ciberdelincuente. Para acceder a la información necesaria, es imprescindible presentar una solicitud formal ante las empresas proveedoras de servicios tecnológicos, las cuales solo pueden responder en virtud de una orden judicial. Este requisito legal, si bien necesario para salvaguardar los derechos fundamentales, genera demoras significativas en la recolección de pruebas digitales, lo cual repercute negativamente en la eficacia de las investigaciones preliminares. Esta situación evidencia la existencia de un sistema procesal poco ágil y desarticulado frente a la dinámica delictiva digital, donde el tiempo es un factor crítico para asegurar la conservación de la evidencia electrónica.

Complementariamente, Animada (2023) sostiene que uno de los principales desafíos para enfrentar el delito informático en el contexto peruano es la ausencia de mecanismos ágiles de interoperabilidad entre las entidades del Estado. La falta de conexión eficiente entre la Policía Nacional, el Ministerio Público, el Poder Judicial y los organismos con competencias tecnológicas limita el intercambio oportuno de información clave, generando dilaciones innecesarias y duplicidad de funciones. A ello se suma la fragmentación normativa, que provoca inconsistencias en la aplicación de las leyes, reduciendo así la efectividad operativa del sistema judicial frente a estos delitos.

En la misma línea, la Defensoría del Pueblo (2023) advierte que la carencia de un protocolo técnico-jurídico uniforme para la recolección, tratamiento y análisis de pruebas digitales debilita gravemente la cadena de custodia. Esta situación afecta el valor probatorio de la evidencia tecnológica, y puede incluso poner en riesgo su admisión en juicio, lo que podría derivar en nulidades procesales o en decisiones prematuras de archivo fiscal. La ausencia de estandarización en los procedimientos deja a los operadores de justicia en una constante

incertidumbre, afectando directamente el principio de legalidad y la tutela efectiva de los derechos vulnerados.

Finalmente, Espinoza (2022) plantea que la persecución penal de los delitos informáticos debe ir acompañada de una reforma estructural e integral, que contemple tanto el fortalecimiento de las capacidades humanas como la modernización de la infraestructura tecnológica de las entidades del sistema de justicia penal. El autor subraya la necesidad de implementar laboratorios forenses digitales, sistemas automatizados de análisis de datos, inteligencia artificial y mecanismos de cooperación internacional en tiempo real. Estas medidas permitirían ofrecer una respuesta penal adecuada y actualizada frente al constante avance tecnológico que caracteriza al fenómeno delictivo digital.

En consecuencia, y tomando en cuenta los vacíos detectados, se hace indispensable una reforma normativa que habilite, bajo estrictos requisitos legales y control judicial, el acceso ágil a la información digital necesaria para las investigaciones. Asimismo, resulta prioritario establecer marcos claros de coordinación interinstitucional, así como protocolos técnicos estandarizados que aseguren la validez, fiabilidad y legalidad de las pruebas recabadas. Solo así el Estado podrá garantizar una respuesta penal efectiva y proteger adecuadamente el bien jurídico de la seguridad digital.

De la misma forma, es posible señalar el **tercer objetivo específico** que es, determinar cuáles serían las medidas correctivas que deberían adoptarse para realizar una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.

Cortés (2015), subraya que la falta de conocimiento técnico forense digital por parte de fiscales y personal de apoyo es una barrera significativa. En ese sentido, propone capacitaciones continuas en herramientas de análisis forense, recuperación de datos y manejo

de la cadena de custodia digital, lo que se alinea directamente con la necesidad de medidas correctivas. En cuanto a los recursos tecnológicos, Zuñiga (2016), enfatiza que las fiscalías deben contar con infraestructura tecnológica de vanguardia, incluyendo software especializado para el análisis de evidencia digital y hardware que permita el almacenamiento seguro y el procesamiento rápido de grandes volúmenes de datos. La carencia de estos recursos, como se infiere de los resultados de una tesis que evalúe la situación actual, impide una investigación ágil y efectiva.

De esa forma, la adecuación del marco normativo es otro pilar fundamental, es así como Pérez (2024), argumenta que, si bien Perú ha avanzado en la tipificación de delitos informáticos, la regulación de procedimientos específicos para la obtención y valoración de la prueba digital aún presenta vacíos. Sugiere la implementación de protocolos claros y estandarizados para la incautación de dispositivos, la preservación de datos en la nube y la validez probatoria de la evidencia electrónica, medidas que serían esenciales para corregir deficiencias actuales.

Complementariamente, Rodríguez (2020), pone en relevancia la importancia de acuerdos interinstitucionales entre la fiscalía, la policía y empresas proveedoras de servicios de internet para agilizar la obtención de información y la ejecución de órdenes judiciales en entornos digitales. De esa forma, la falta de estos acuerdos o la ineficacia de los existentes requeriría medidas correctivas enfocadas en la cooperación y la interoperabilidad.

Siguiendo esa línea, Matallana (2020), especifica que los delitos informáticos rara vez se circunscriben a una sola jurisdicción. Postula la necesidad de fortalecer los canales de comunicación y coordinación entre las fiscalías especializadas, la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú, y otras entidades relevantes.

En ese orden de ideas, Pérez (2023), aboga por la intensificación de la participación de las fiscalías peruanas en redes de cooperación internacional, como la Red Iberoamericana de Fiscales Especializados en Cibercrimen (RIFCE) o el Convenio de Budapest sobre Ciberdelincuencia. La implementación de medidas correctivas en este ámbito implicaría la capacitación en mecanismos de asistencia judicial internacional y la promoción de convenios bilaterales o multilaterales que faciliten la persecución de estos delitos. En resumen, los autores citados convergen en la necesidad de abordar las deficiencias actuales mediante el fortalecimiento de capacidades técnicas y tecnológicas, la actualización y estandarización del marco normativo y los protocolos de actuación, y la mejora sustancial de la cooperación interinstitucional e internacional.

VI. CONCLUSIONES

6.1 La investigación fiscal desempeña un papel clave en la efectividad de la sanción de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia. Cuando se aplican técnicas forenses digitales adecuadas, el personal está capacitado y se cuenta con recursos tecnológicos suficientes, aumenta la capacidad de los fiscales para reunir pruebas sólidas, identificar a los responsables y sustentar casos que concluyan en condenas. En cambio, la falta de preparación o de medios técnicos limita la eficacia de las investigaciones, reduce la tasa de sanciones y favorece la impunidad, lo que también desalienta a las víctimas a denunciar estos delitos.

6.2 Las limitaciones para una persecución efectiva de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia de Lima Centro responden a múltiples factores. Entre ellos destacan la insuficiente capacitación de fiscales y policías en investigación digital, la falta de infraestructura tecnológica actualizada y la ausencia de protocolos claros para garantizar la cadena de custodia de la evidencia digital. También influye la complejidad de los ciberdelitos, que suelen tener un carácter transnacional y evolucionar rápidamente, así como la escasa coordinación entre instituciones nacionales y organismos internacionales para el intercambio y obtención de pruebas.

6.3 La ausencia de identificación de los implicados en delitos informáticos acarrea serias repercusiones para el desarrollo de una investigación fiscal efectiva en las Fiscalías Especializadas de Ciberdelincuencia. Esta falencia impide asignar responsabilidades penales, lo que favorece la impunidad y vulnera el principio de justicia. Además, provoca desconfianza en el sistema judicial, desalienta a las víctimas a denunciar y fomenta la reincidencia al percibirse un bajo riesgo de sanción. También obstaculiza el desmantelamiento de organizaciones criminales y la recuperación de bienes obtenidos ilícitamente.

6.4 Para realizar una investigación fiscal efectiva de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia de Lima Centro, es imprescindible tomar medidas correctivas como la inversión en tecnología forense avanzada, la formación constante y especializada del personal fiscal y de apoyo en ciberdelincuencia, además de desarrollar protocolos uniformes y precisos para la recolección, conservación y análisis de las pruebas digitales. También es esencial potenciar la colaboración entre instituciones, tanto con la Policía Nacional del Perú como con otras entidades significativas, además de promover la cooperación internacional para encarar el carácter transfronterizo de estos crímenes, asegurando de este modo una persecución penal más eficaz y un castigo apropiado a los culpables.

VII. RECOMENDACIONES

7.1 Al Ministerio del Interior

Incrementar el presupuesto para ampliar más recursos humanos y logísticos de la División de Investigación de Alta Tecnología que depende de la Dirección de Investigación Criminal de la Policía Nacional del Perú, a fin de hacer una persecución eficaz de dicha modalidad delictiva, sobre todo en las actividades de diligencia preliminares e incrementar el presupuesto para ampliar más recursos humanos y logísticos de la Fiscalía de ciberdelincuencia en Lima, a fin de hacer una persecución eficaz de dicha modalidad delictiva, sobre todo en las actividades de diligencia preliminares.

7.2 A la Superintendencia de Banca y Seguros

Realizar difusiones masivas a los usuarios de las entidades financieras sobre actividades de prevención frene a los delitos de ciberdelincuencia a efectos de concientizar en la ciudadanía el cuidado respectivo.

7.3 Al Poder Judicial

Fomentar la capacitación especializada de jueces y personal jurisdiccional en materia de delitos informáticos y evidencia digital, a fin de garantizar una valoración probatoria adecuada y la emisión de sentencias que reflejen la complejidad y particularidades de esta modalidad delictiva. Esto incluye la actualización sobre nuevas tecnologías, criptografía y técnicas forenses digitales, asegurando así un conocimiento profundo para la administración de justicia.

7.4 A las Universidades y Centros de Investigación

Promover la creación y fortalecimiento de programas académicos, cursos de especialización e investigaciones en ciberseguridad, derecho informático y forense digital. Esto contribuiría a formar profesionales con las competencias necesarias para enfrentar los desafíos

de los delitos informáticos, proveyendo al sistema de justicia y a la sociedad en general de expertos capacitados para la prevención, detección e investigación de estos ilícitos.

VIII. REFERENCIAS

Acosta, M. G., Benavides, M. M. y García, N. P. (2020) *Delitos informáticos: Impunidad organizacional y su complejidad en el mundo de los negocios*. Revista Venezolana de Gerencia, 25(89). Universidad del Zulia. https://www.redalyc.org/journal/290/29062641023/html/

Animaca, Y. A. (2023). Delitos informáticos y la ciberdelincuencia con el uso de las nuevas tecnologías en Lima Centro 2022 [Tesis de maestría, Universidad César Vallejo] Repositorio de la Universidad Cesar Vallejo. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/122811/Anicama_AYA-SD.pdf? sequence=1&isAllowed=yfgfgf

Ayma, H. (2020). *Delitos informáticos y su relación con el proceso de investigación preliminar en el Distrito Fiscal de Lima Norte año 2019* [Tesis de posgrado, Universidad Alas Peruanas]. Repositorio UAP. https://repositorio.uap.edu.pe/bitstream/handle/20.500.12990/6216/Delitos%20inform%C3%A1ticos_Relaci%C3%B3n_Proceso%20de%20investigaci%C3%B3n%20preliminar.pdf?sequence=1&isAllowed=y

Ballesteros, M. C., & Gómez, J. A. (2014). Cibercrimen: particularidades en su investigación y enjuiciamiento. *Anuario Jurídico Y Económico Escurialense*, (47), 209–234. Recuperado a partir de https://publicaciones.rcumariacristina.net/AJEE/article/view/189

Barrio, M. (2017a). Ciberdelitos. Amenazas criminales del ciberespcio. Reus.

Binder, A. M. (2012). *Introducción al proceso penal acusatorio*. Ad-Hoc.

Brenner, S. W. (2010). *Cybercrime: Criminal threats from cyberspace*. https://www.researchgate.net/publication/266090469_Cybercrime_Criminal_Threats_from_Cyberspace

Carrillo Díaz, C., & Montenegro Dávila, A. (2018). *La criminalidad informática o tecnológica y sus deficiencias legislativas en el delito de atentado a la integridad de sistemas informáticos*. https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/4514/Carrillo%20Diaz%20%26%20Montenegro%20Davila.pdf

Chavarría, G. R. (2023) *Delitos informáticos y la implementación de la Unidad Fiscal Especializada en Ciberdelincuencia del Ministerio Público en el Perú.* [Tesis de maestría, Universidad Cesar Vallejo] Repositorio Institucional Universidad Cesar Vallejo. https://hdl.handle.net/20.500.12692/129744

Chávez, E. (2018) El delito contra datos y sistemas informáticos en el derecho fundamental a la intimidad personal en la corte superior de justicia de lima norte, 2017. [Tesis de magister Universidad Nacional Federico Villareal] Disponible en el repositorio de la Institución. https://hdl.handle.net/20.500.13084/2704

Clavijo Velasco, J. (2015). *Delitos informáticos: Enfoque jurídico penal y procesal*. Bogotá: Editorial Ibáñez.

Cortés, R. (2015). *La persecución penal de delitos informáticos: Desafíos y propuestas para la justicia digital*.

Defensoría del Pueblo (2023). La ciberdelincuencia en el Perú: estrategias delictivas. Instituto Pacífico.

Díaz, C. (2019) La aplicación de la ley Nº. 30096 -Ley de delitos informáticos respecto a su regulación en el derecho penal peruano. [Tesis de pregrado, Cesar Vallejo] Disponible en el repositorio de la Institución. https://hdl.handle.net/20.500.12692/51569

Espinoza Calderón, V. R. (2022). Delitos informáticos y nuevas modalidades

Espinoza, V. (2022). Análisis de los delitos informáticos y el valor probatorio de la evidencia digital en la Corte Superior de Justicia de

Estrada Salvador, C. (2024). La impunidad en los delitos informáticos. Una problemática de poco interés por los legisladores, jueces y fiscales. *Ius Vocatio, 7*(9), Art. 928. https://doi.org/10.35292/iusVocatio.v7i9.928

Flores, L. L. (2014). Derecho informático. Patria.

Gómez, L. (2024). *Diligencias preliminares y su incidencia en la persecución eficaz de los delitos informáticos en el Distrito Fiscal de Lima Sur, 2021-2022* [Tesis de pregrado, Universidad Privada San Juan Bautista]. Repositorio UPSJB. https://repositorio.upsjb.edu.pe/bitstream/handle/20.500.14308/5361/TI-MDPP-GOMEZ%20VELASQUEZ%20LIZBETH%20MILABE.pdf?sequence=1&isAllowed=y

González Cussac, J. L. (2010). *Delitos informáticos y prueba electrónica*. Tirant lo Blanch. handle/20.500.12692/122811/Anicama_AYA-SD.pdf? sequence=

Hernández, N. & Patricio, A. (2022). *La obtención de pruebas en delitos cibernéticos en las Fiscalías Especializadas en Ciberdelincuencia de Lima Centro 2021* [Tesis de pregrado, Universidad César Vallejo]. Repositorio UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/88754/Hern%C3%A1ndez_AN-Patricio_RAE-SD.pdf?sequence=1

Herrera, L. (2018) Eficacia de la ley de delitos informáticos en el distrito judicial de Huánuco 2017. [Tesis de pregrado, Universidad de Huánuco] Disponible en el repositorio de la Institución. http://repositorio.udh.edu.pe/123456789/1058

Jiménez, J. C. (2017) Manual de derecho informático. *Jurista Editores.*

López, D. (2023) Investigación policial de la ciberdelincuencia y capacidad de respuesta de la Policía Nacional en materia de formación y capacitación a través del Proyecto C1b3rWall. [Tesis de Doctorado, Universidad de Salamanca] http://hdl.handle.net/10366/158077

Martínez (2020) J. (2020). *Los delitos informáticos en el ordenamiento jurídico peruano*. Revista Derecho & Sociedad, (54), 113–125.

Martínez, J. (2021). *Actuación de los Ministerios Públicos ante las denuncias y querellas en materia de delitos informáticos en Guerrero en el 2020* [Tesis de posgrado, Universidad Autónoma de Guerrero]. Repositorio UAGro. http://ri.uagro.mx/bitstream/handle/uagro/3148/TM_8039997_21.pdf?sequence=1&isAllowed=y

Matallana, R. (2020). Desafíos y oportunidades de la justicia digital en el ámbito laboral 10.47308/rdpt. v2i2.4

Matos, E. (2022) Especialización de la investigación preparatoria en los delitos de fraudes informáticos. [Tesis de grado Universidad Cesar Vallejo] Disponible en el repositorio de la Universidad. https://hdl.handle.net/20.500.12692/84087

Mendoza García, L. (2017). *Criminalidad informática y derecho penal*. Lima: Palestra Editores.

Milla, L. (2021) *El Delito Informático y su Deficiencias Legislativas.* [Tesis de grado, Universidad San Andrés. USAN] Repositorio de la Universidad San Andrés. http://repositorio.usan.edu.pe/handle/usan/150

Ministerio Público. (2021, febrero 22). *Nueva Unidad Fiscal Especializada En Ciberdelincuencia inició sus funciones*. Plataforma del Estado Peruano. https://www.gob.pe/institucion/mpfn/noticias/343392-nueva-unidad-fiscal-especializada-en-ciberdelincuencia-inicio-sus-funciones

Ministerio Público. (2023). *Informe anual de gestión institucional 2023*. https://www.mpfn.gob.pe/documentos/informes/Informe_Gestion_2023.pdf

Nivelo, E. (2021). *Tratamiento de los delitos informáticos en el código orgánico integral penal*. Universidad Regional Autónoma de los Andes.

https://dspace.uniandes.edu.ec/bitstream/123456789/14110/1/USD-DEREAC-090-2021.pdf

Orellano, G. y Galindo, S. (2024) Deficiencias legislativas en el tratamiento de la Ley N° 30096, Ley de delitos informáticos – fraude informático, Lima 2019 – 2021. [Tesis de grado, Universidad Cesar Vallejo] Disponible en el repositorio de la Universidad. https://hdl.handle.net/20.500.12692/102672

Pardo, A. (2018) Tratamiento jurídico penal de los delitos informáticos contra el patrimonio, Distrito Judicial de Lima, 2018 [Tesis de maestría, Universidad Cesar Vallejo] Disponible en el repositorio de la Institución. https://hdl.handle.net/20.500.12692/20372

Peralta, R. Los delitos informáticos y los datos en sistemas informáticos [Tesis de grado, Universidad Peruana de Las Américas] Disponible en el repositorio de la Universidad. http://repositorio.ulasamericas.edu.pe/handle/upa/2572

Pérez, A. (2024). *Derecho penal informático: Aspectos sustantivos y procesales en la era digital*.

Ponds, V. (2017) Internet, la nueva era del delito: ciberdelito, ciberterrorismo, legislación y ciberseguridad. Flacso. https://www.redalyc.org/journal/5526/552656641007/html/

Prado Saldarriaga, V. (2016). *El Ministerio Público y los desafíos del proceso penal acusatorio*. Fondo Editorial del Poder Judicial del Perú.

Ramos, L. (2014). *Derecho procesal penal: Principios y práctica*. Fondo Editorial PUCP.

Rodríguez, M. (2020). Ciberseguridad y el sistema de justicia: La necesidad de una modernización urgente. *Revista de Derecho y Nuevas Tecnologías*, *Volumen*, https://www.redalyc.org/journal/5537/553770600002/html/

Rosales, R. (2025) Incremento de los delitos informáticos y su problemática con la impunidad delictiva en Lima, 2024. [Tesis de pregrado, Autónoma Universidad del Perú] Disponible en el repositorio de la Institución. https://hdl.handle.net/20.500.13067/3793

Sánchez, J. (2018) Delitos informáticos. In. B. M. (Ed.) Ciberseguridad y ciberdefensa (pp. 31-52) *Dykinson.*

Sánchez, K. (2019). *La tipificación del delito de acceso ilícito a sistemas y equipos de informática en México* [Tesis de posgrado, Universidad Autónoma de Sinaloa]. Repositorio UAS. https://derecho.uas.edu.mx/posgrado/documentos/MCD6G/SanchezVillaKarlaKarina.pdf

Schirakian, N. (2021). *Evidencia informática: ¿Un nuevo paradigma para el derecho procesal penal?* [Tesis de posgrado, Universidad San Andrés]. Repositorio UDESA. https://repositorio.udesa.edu.ar/jspui/bitstream/10908/18968/1/%5BP%5D%5BW%5D%20M.%20Der.%20Penal%20Schirakian%2C%20Natalia.pdf

Silva Sánchez, J. M. (2012). *La expansión del derecho penal: aspectos de la política criminal en las sociedades postindustriales*. Madrid: Thomson Reuters-Civitas.

Sotomayor, G. (2022) La calificación fiscal en los delitos informáticos en el distrito fiscal de Lima Centro, 2019 – 2020. [Tesis de Maestría, Universidad Cesar Vallejo] Disponible en el repositorio de la Universidad. https://hdl.handle.net/20.500.12692/95834

Sotomayor. (2022). *La calificación fiscal en los delitos informáticos en el Distrito Fiscal de Lima Centro, 2019–2020* [Tesis de posgrado, Universidad César Vallejo]. Repositorio UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/95834/Sotomayor_RGB-SD.pdf?sequence=4&isAllowed=y

Tejada, E. (2017). Novedades en la tipificación de determinados delitos vinculados a la criminalidad informática en el Código Penal español: evolución legislativa y adaptación a la normativa internacional. En D. Dupuy (dir.) y M. Kiefer (coord.), Cibercrimen.Aspectos de derecho penal y procesal penal. Cooperación internacional. Recolección de evidencia digital. Responsabilidad de los proveedores de servicio de internet (pp. 33-57). BdeF.

Ticse Baquerizo, A. (2025, junio 9). *Se regula el uso de la tecnología digital en la remisión de la carpeta fiscal, en la declaración del imputado y en las diligencias de la investigación preparatoria*. Actualidad Empresarial. https://actualidadempresarial.pe/comentario-legal/se-regula-el-uso-de-la-tecnologia-digital-en-la-remision-de-la-carpeta-fiscal-en-la-declaracion-del-imputado-y-en-las-diligencias-de-la-investigacion-preparatoria/1

Toledo, I. Y Venegas, L. (2020) Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional. [Tesis de grado Universidad de Chile] Disponible en el repositorio de la Institución. https://repositorio.uchile.cl/handle/2250/176344

Torres F. (2019) La tipificación de los delitos informáticos y su contextualización con el sistema digital y tecnológico. [Tesis de grado, Universidad de Santander (UDES] Disponible en el repositorio de la Institución https://repositorio.udes.edu.co/handle/001/4422

Torres, C. (2019) La investigación de los delitos ambientales y el nivel de pronunciamiento por la fiscalía especializada del distrito fiscal de Pasco – periodo 2018. [Tesis de pregrado, Universidad Nacional Daniel Alcides Carrión] Disponible en el repositorio de la Institución. http://repositorio.undac.edu.pe/handle/undac/2208

Universidad Nacional Federico Villarreal (UNFV). (2023). *Desafíos para el procesamiento de los delitos informáticos en una fiscalía de Lima Este, 2023* [Tesis de licenciatura].

Repositorio Institucional de la Universidad Nacional Federico Villarreal. https://repositorio.unfv.edu.pe/handle/20.500.13084/10677

Usaqui, K. (2022). *Los actos de investigación en la persecución eficaz de los delitos cometidos por la ciberdelincuencia, Distrito Fiscal de Lima, 2021* [Tesis de posgrado, Universidad César Vallejo]. Repositorio UCV. https://repositorio.ucv.edu.pe/bitstream/handle/20.500.12692/89325/Usaqui_BK-SD.pdf?sequence=1&isAllowed=y

Villavicencio Terreros, F. (2014). Delitos Informáticos. *IUS ET VERITAS*, *24*(49), 284-304. Recuperado a partir de https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/13630

Zaffaroni, E. R., Alagia, A., & Slokar, A. (2011). *Derecho procesal penal*. Ediar.

Zavala, A. (2018). *Ciberdelitos en el Perú: Comentarios a la Ley N.º 30096*. Gaceta Jurídica. Autor peruano que comenta la ley de delitos informáticos, con enfoque doctrinario y análisis práctico de casos nacionales.

Zuñiga, M. (2016). *Criminalidad organizada transnacional en el ámbito digital: Un análisis desde la perspectiva jurídica*.

IX. ANEXOS

Anexo A: Matriz de Consistencia

PROBLEMAS	OBJETIVOS	HIPOTESIS	CATEGORÍAS	MÉTODO
Problema general ¿Cómo influye la investigación fiscal en la eficacia de la sanción de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024? ***Problemas específicos*** **1.** ¿Cuáles son las causas que limitan realizar una persecución eficaz de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024? **2.** ¿Cuáles son las consecuencias que conlleva la falta de identificación de los partícipes del delito informático para garantizar una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024? **3.** ¿Cuáles serían las medidas correctivas que deberían adoptarse para realizar una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024?	***Objetivo general*** Determinar cómo influye la investigación fiscal en la eficacia de la sanción de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024. ***Objetivos específicos*** **O.1.** Determinar cuáles son las causas que limitan realizar una persecución eficaz de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024. **O.2.** Determinar las cuáles son las consecuencias que conlleva la falta de identificación de los partícipes del delito informático para garantizar una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024. **O.3.** Determinar cuáles serían las medidas correctivas que deberían adoptarse para realizar una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.	***Hipótesis general*** La investigación fiscal influye en la eficacia de la sanción de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024. ***Hipótesis específicas*** **H.1.** La falta de capacitación fiscal, actualización digital de los despachos, falta de actividad probatoria que permita identificar el sujeto del delito se relacionan como causas que afectan la investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024. **H.2.** La ineficacia de la investigación fiscal de los delitos informáticos ocasiona la falta de identificación de los partícipes del delito; en consecuencia, se archiven definitivamente las denuncias penales en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024. **H.3.** La implementación de medidas correctivas permitiría una eficaz investigación fiscal de los delitos informáticos en las Fiscalías Especializadas de Ciberdelincuencia en Lima Centro, 2024.	EFICACIA DE LA INVESTIGACIÓN FISCAL **Subcategorías** ● Causas de la ineficacia de la investigación fiscal ● Consecuencias de la ineficacia de la investigación fiscal ● Medidas correctivas para mejorar la investigación fiscal del delito DELITOS INFORMÁTICOS **Subcategorías** ● Diligencias preliminares en delitos informáticos ● Actividades probatorias ● Identificación del sujeto activo	**Método de investigación:** Cualitativo **Tipo de Investigación:** Básica **Nivel de Investigación**: Descriptivo - Explicativo **Diseño:** No experimental **Muestra:** No probalistica **Instrumentos:** - Guia de Entrevistas - Análisis documental

Anexo B: Matriz de Categorización

VARIBLES	DEFINICIÓN DE VARIABLES	SUBCATEGORÍAS	DEFINICIÓN DE SUBCATEGORÍAS
EFICACIA DE LA INVESTIGACIÓN FISCAL	Saldarriaga (2005) Saldarriaga destaca que la eficacia de la investigación fiscal no depende únicamente de la formalización de la denuncia o la acusación, sino de una labor investigativa oportuna, estratégica y bien articulada con la policía y demás órganos del sistema de justicia, con el fin de evitar impunidad y asegurar la tutela efectiva de los derechos fundamentales.	Causas de la ineficacia de la investigación fiscal	Binder (2012) indica que la ineficacia fiscal muchas veces se origina en una cultura jurídica inquisitiva aún arraigada, en deficiencias organizativas del Ministerio Público y en la ausencia de una política criminal clara que oriente la actuación fiscal.
		Consecuencias de la ineficiencia de la investigación fiscal.	Ramos, L. (2014) señala que la ineficiencia en la investigación fiscal conlleva consecuencias graves como la prolongación de los procesos judiciales, la impunidad de los responsables, la vulneración del derecho de las víctimas a la justicia y el debilitamiento de la confianza ciudadana en el sistema de administración de justicia
		Medidas correctivas para mejorar la investigación fiscal del delito.	Zaffaroni (2011) señala la necesidad de crear unidades especializadas dentro del Ministerio Público para delitos complejos, así como garantizar autonomía y recursos para que la investigación fiscal sea más eficiente y efectiva.
DELITOS INFORMÁTICOS	Define a los delitos informáticos como aquellas acciones ilícitas realizadas mediante sistemas informáticos, que afectan la confidencialidad, integridad y disponibilidad de la	Diligencias preliminares en delitos informáticos	García (2014) Alega que las diligencias preliminares en delitos informáticos constituyen el conjunto de actuaciones iniciales que realiza el Ministerio Público para verificar la existencia de un hecho delictivo, determinar la presunta comisión del delito y recolectar indicios esenciales antes de formalizar la investigación penal. Estas diligencias buscan preservar la evidencia digital y evitar su alteración o pérdida debido a la naturaleza volátil de los medios tecnológicos.

	información, conforme a la tipificación establecida en la Ley N.º 30096. Asimismo, los delitos informáticos comprenden un conjunto heterogéneo de conductas delictivas donde el uso de las TIC es esencial, ya sea como herramienta para cometer el delito o como objeto del ataque.	Actividades probatorias	En el contexto de los delitos informáticos, las actividades probatorias adquieren especial relevancia, pues implican técnicas especializadas como la preservación de evidencia digital y la realización de peritajes forenses informáticos, como señala González Cussac (2010)**,** quien destaca la importancia de garantizar la integridad y autenticidad de los datos para que sean válidos en el proceso penal.
		Identificación del sujeto activo.	Según Binder (2012), la identificación implica no solo señalar al individuo, sino también demostrar su participación directa o indirecta en la conducta delictiva, basada en evidencias concretas. En el contexto de los delitos informáticos, la identificación del sujeto activo presenta retos particulares debido al uso de tecnologías que permiten el anonimato o la suplantación de identidad, por lo que es necesaria la aplicación de técnicas especializadas de investigación digital.

Anexo C: Guías de entrevista aplicadas

Universidad Nacional Federico Villarreal

Guía de entrevista

Título: "EFICACIA DE LA INVESTIGACIÓN FISCAL DE LOS DELITOS INFORMÁTICOS EN LAS FISCALÍAS ESPECIALIZADAS EN CIBERDELINCUENCIA DE LIMA CENTRO, 2024."

Entrevistadora: PAOLA VANESSA CHARAJA COA TA

Profesión: ABOGADA

Grado académico: MAGISTER.

Cargo: FISCAL PROVINCIAL TITULAR

Institución donde labora: Ministerio Público-Despacho de la Ciberdelincuencia.

Indicaciones: Se le pide responder a las preguntas de manera más objetiva posible, pues los datos que mencione son de gran valor e interés para el presente trabajo.

Preguntas:

1. **De acuerdo con su experiencia ¿Cuál es el impacto del delito informático en nuestra ciudad? Explique Ud.**

Impacta en diferentes áreas, en la confianza del sistema financiero a nivel del patrimonio de los ciudadanos

y la seguridad digital y otros.

2. **De acuerdo con su experiencia ¿Considera que la conducta de la víctima contribuye a la perpetración del delito informático? Explique Ud.**

Sí, ya que en muchos delitos informáticos es necesario para su perpetración el error humano, donde los

ciberdelincuentes aprovechas dicho error para ingresar obtener sus claves o irrumpir en su entorno digital.

3. **De acuerdo con su experiencia ¿Considera que la conducta de las entidades financieras en caso de fraude tarjetas de crédito contribuye a la perpetración del delito informático? Explique Ud.**

Sí, en algunos casos las medidas de validación no son lo suficientemente seguras, lo que facilita suplantaciones de identidad, en otros casos el personal.

4. **De acuerdo con su experiencia ¿Cuáles son las implicancias que conlleva falta de identificación de los partícipes del delito informático? Explique Ud.**

Conlleva al archivo de las denuncias o la impunidad de algunos de los implicados del hecho.

5. En su opinión ¿Cuáles las medidas correctivas que deben adoptarse para hacer una persecución eficaz al delito informático? Explique Ud.

1. La especialidad es indispensable, es decir la capacitación especializada del investigador. 2. El apoyo adecuado por parte de las instituciones financieras y telecomunicaciones para brindar la información requerida. 3. La preservación de la evidencia digital y otros.

Firma del participante

Nombre: PAOLA VANESSA CHARAJA COATA

Fecha: 16/04/2025

PAOLA VANESSA CHARAJA COATA
Fiscal Provincial (T)
Primera Fiscalía Corporativa Especializada
en Ciberdelincuencia de Lima centro
Quinto Despacho Provincial

Universidad Nacional Federico Villarreal

Guía de entrevista

Título: "EFICACIA DE LA INVESTIGACIÓN FISCAL DE LOS DELITOS INFORMÁTICOS EN LAS FISCALÍAS ESPECIALIZADAS EN CIBERDELINCUENCIA DE LIMA CENTRO, 2024."

Entrevistadora: Elsa Lisbeth Sánchez Gutiérrez.

Profesión: Abogada

Grado académico: Magister.

Cargo: Fiscal Adjunto Provincial

Institución donde labora: Ministerio Público.

Indicaciones: Se le pide responder a las preguntas de manera más objetiva posible, pues los datos que mencione son de gran valor e interés para el presente trabajo.

Preguntas:

1. De acuerdo con su experiencia ¿Cuál es el impacto del delito informático en nuestra ciudad? Explique Ud.

El delito informático ha ido en aumento junto con el avance de la tecnología, lo cual ocasiona nuevas modalidades de incurrir en ellos y estando a su realización por medios digitales es más complejo su persecución.

2. De acuerdo con su experiencia ¿Considera que la conducta de la víctima contribuye a la perpetración del delito informático? Explique Ud.

Depende de la modalidad del delito, existen algunas modalidades como el phishing o el vishing que son bastantes conocidos y difundidos por medios periodísticos con la finalidad de prevenirlos, sin embargo, pese a ello, la población no se informa e incurre de forma reiterada en estas modalidades delictivas. Por otro lado, existen otros delitos que requieren un acceso ilícito a sistemas, para su comisión y por más cuidados que la víctima pueda tener, se está expuesta a ellos.

3. De acuerdo con su experiencia ¿Considera que la conducta de las entidades financieras en caso de fraude tarjetas de crédito contribuye a la perpetración del delito informático? Explique Ud.

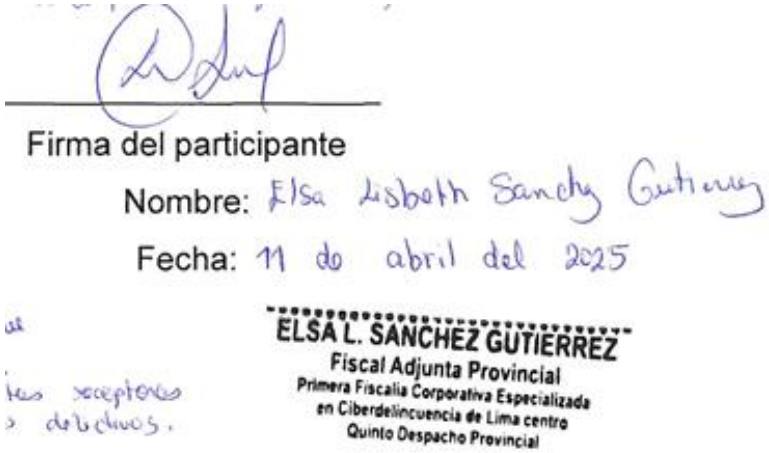
En cierta medida, debido a que no implementan mecanismos de seguridad relacionadas al uso de las tarjetas en los comercios, como por ejemplo contar con un CVV virtual y no físico.

4. De acuerdo con su experiencia ¿Cuáles son las implicancias que conlleva falta de identificación de los partícipes del delito informático? Explique Ud.

La principal es la impunidad, debido a que no se logra una sanción penal para ello, así como tampoco prevenir su participación en hechos similares, y, por otro lado, el hecho de que el agraviado no conozca quien se apoderó de su dinero y no vea satisfecho el perjuicio ocasionado.

5. En su opinión ¿Cuáles las medidas correctivas que deben adoptarse para hacer una persecución eficaz al delito informático? Explique ud

-Garantizar que la información no sea tan volátil y que pese el tiempo transcurrido aun pueda obtenerse (IPS, información bancaria, cámaras de seguridad, información comercial) copias espejo de dispositivos afectados, etc. 2.- Implementar mesas de trabajo tanto con las empresas operadoras bancarias y demás que participan en brindar información con la finalidad de garantizar una respuesta optima, rápida y de acuerdo con lo solicitado. 3. Implementar bases de datos que permitan compartir información a nivel fiscal sobre nombres de cuentas receptoras y demás partícipes en estos hechos delictivos.



Universidad Nacional Federico Villarreal

Título: "EFICACIA DE LA INVESTIGACIÓN FISCAL DE LOS DELITOS INFORMÁTICOS EN LAS FISCALÍAS ESPECIALIZADAS EN CIBERDELINCUENCIA DE LIMA CENTRO, 2024."

Entrevistadora: María Sánchez Loayza.

Profesión: Abogada

Grado académico: Magister.

Cargo: Fiscal Adjunto Provincial de Fiscalía Ciberdelincuencia Lima Centro.

Institución donde labora: Ministerio Público.

Indicaciones: Se le pide responder a las preguntas de manera más objetiva posible, pues los datos que mencione son de gran valor e interés para el presente trabajo.

Preguntas:

1. De acuerdo con su experiencia ¿Cuál es el impacto del delito informático en nuestra ciudad? Explique Ud.

A raíz del COVID 19, donde la virtualidad estuvo en todo su auge se pudo advertir el incremento de estos delitos informáticos, el cual se ha visto perfeccionado, dado que son delitos donde prima el anonimato.

2. De acuerdo con su experiencia ¿Considera que la conducta de la víctima contribuye a la perpetración del delito informático? Explique Ud.

Claro que sí, ya que el desconocimiento de los agraviados en no brindar sus confidenciales bancarios y a

ingresar a enlaces falsos- fishing, es el común de los delincuentes para cometer delitos ilícitos

3. De acuerdo con su experiencia ¿Considera que la conducta de las entidades financieras en caso de fraude tarjetas de crédito contribuye a la perpetración del delito informático? Explique Ud.

Creo que el banco no contribuye a la perpetración del delito, ya que son los usuarios los responsables del uso tarjetas, pero si considero que su rechazo de los bancos y la mala información contribuyen a la no identificación de los investigados.

4. De acuerdo con su experiencia ¿Cuáles son las implicancias que conlleva falta de identificación de los partícipes del delito informático? Explique Ud.

1.- Que los policías no solicitan información de cámaras o no la recaban cuando se pone denuncia. 2.- Que el banco demora en remitir respuesta y no resguardan cámaras. 3.- Que el banco no informa los datos de los comercios donde realizaron operaciones no reconocidas.

5. En su opinión ¿Cuáles las medidas correctivas que deben adoptarse para hacer una persecución eficaz al delito informático? Explique Ud.

1.-El banco asuma la deuda cuando no valida los datos correctamente, por parte de la SBS, que reciba sanción frente al incumplimiento. 2.- Que sanciones a las empresas telefónicas por no tener filtros correspondientes para evitar suplantación de identidad, por parte de OSIPTEL reciba sanción frente al incumplimiento.

Firma del participante

Nombre: Paola Maria Sanchez Lozano

Fecha: 07/04/2025

Universidad Nacional Federico Villarreal

Guía de entrevista

Título: "EFICACIA DE LA INVESTIGACIÓN FISCAL DE LOS DELITOS INFORMÁTICOS EN LAS FISCALÍAS ESPECIALIZADAS EN CIBERDELINCUENCIA DE LIMA CENTRO, 2024."

Entrevistadora: Ángel Gonzales Farfán.

Profesión: Abogado

Grado académico: Magister.

Cargo: Fiscal Adjunto Provincial de Fiscalía Ciberdelincuencia Lima Centro.

Institución donde labora: Ministerio Público.

Indicaciones: Se le pide responder a las preguntas de manera más objetiva posible, pues los datos que mencione son de gran valor e interés para el presente trabajo.

Preguntas:

1. De acuerdo con su experiencia ¿Cuál es el impacto del delito informático en nuestra ciudad? Explique Ud.

Negativo y múltiple pues puede considerárseles como pluriofensivo, al comprometer varios bienes jurídicos protegidos: patrimonio, identidad, intimidad, seguridad, indemnidad sexual, etc.

2. De acuerdo con su experiencia ¿Considera que la conducta de la víctima contribuye a la perpetración del delito informático? Explique Ud.

No por su conducta, aunque sí pro su "condición", debido a la brecha digital, no todos son conscientes de la importancia de la ciberseguridad al momento de utilizar las tecnologías de la información y la comunicación (TIC).

3. De acuerdo con su experiencia ¿Considera que la conducta de las entidades financieras en caso de fraude tarjetas de crédito contribuye a la perpetración del delito informático? Explique Ud.

Si se verifica o demuestra que, una entidad "omite" velar por el incremento de sus niveles de ciberseguridad, quizás sí podría informar que esa omisión contribuye a la perpetración del delito.

4. De acuerdo con su experiencia ¿Cuáles son las implicancias que conlleva falta de identificación de los partícipes del delito informático? Explique Ud.

La propia naturaleza del entorno digital de los delitos informáticos, que lo convierten en delitos con entornos furtivos o clandestinos.

5. En su opinión ¿Cuáles las medidas correctivas que deben adoptarse para hacer una persecución eficaz al delito informático? Explique Ud.

Acceder a la información administrada por el sector privado (bancario /comunicaciones) en tiempo casi real.

Universidad Nacional Federico Villarreal

Guía de entrevista

Título: "EFICACIA DE LA INVESTIGACIÓN FISCAL DE LOS DELITOS INFORMÁTICOS EN LAS FISCALÍAS ESPECIALIZADAS EN CIBERDELINCUENCIA DE LIMA CENTRO, 2024."

Entrevistadora: Gianina Imelda Orozco Huainani

Profesión: Abogado

Grado académico: Magister.

Cargo: Fiscal Adjunto Provincial de Fiscalía Ciberdelincuencia Lima Centro.

Institución donde labora: Ministerio Público.

Indicaciones: Se le pide responder a las preguntas de manera más objetiva posible, pues los datos que mencione son de gran valor e interés para el presente trabajo.

Preguntas:

1. De acuerdo con su experiencia ¿Cuál es el impacto del delito informático en nuestra ciudad? Explique Ud.

Positivo y Negativo, ya que al obtener el avance tecnológico se puede garantizar optimo avance para la seguridad informática; negativo debido que no todos manejan con responsabilidad el uso de las TIC

2. De acuerdo con su experiencia ¿Considera que la conducta de la víctima contribuye a la perpetración del delito informático? Explique Ud.

Sí, porque con el avance de la tecnología la población no se encuentra informada que, ante cualquier error en la introducción de sus datos personales o el contenido de sus tarjetas, los ciberdelincuentes aprovechan generándoles un perjuicio económico.

3. De acuerdo con su experiencia ¿Considera que la conducta de las entidades financieras en caso de fraude tarjetas de crédito contribuye a la perpetración del delito informático? Explique Ud.

Si, porque muchas veces sus medidas de seguridad son vulneradas, al no obtener un manejo responsable como entidad financiera, y el uso poco responsable de sus usuarios.

4. De acuerdo con su experiencia ¿Cuáles son las implicancias que conlleva falta de identificación de los partícipes del delito informático? Explique Ud.

Archivos de denuncias, impunidad para algunos responsables del hecho, el banco no remite información detallada que permita coadyuvar al esclarecimiento del hecho.

5. En su opinión ¿Cuáles las medidas correctivas que deben adoptarse para hacer una persecución eficaz al delito informático? Explique Ud.

Capacitaciones especializadas en ciberseguridad, el apoyo eficaz del sector privado y público para obtener información en tiempo y espacio real.

Firma del participante

Nombre: Yanina Imelda Orozco Huayanay

Fecha: 14/04/2025

Yanina Imelda Orozco Huayanay
Fiscal Provincial
4° Despacho Provincial de la 2° Fiscalía Corporativa
Especializada en Ciberdelincuencia de Lima Centro

Universidad Nacional
Federico Villarreal

Guía de entrevista

Título: "EFICACIA DE LA INVESTIGACIÓN FISCAL DE LOS DELITOS INFORMÁTICOS EN LAS FISCALÍAS ESPECIALIZADAS EN CIBERDELINCUENCIA DE LIMA CENTRO, 2024."

Entrevistadora: Lery Rojas Huaino

Profesión: Abogado

Grado académico: Magister.

Cargo: Fiscal Adjunto Provincial de Fiscalía Ciberdelincuencia Lima Centro.

Institución donde labora: Ministerio Público.

Indicaciones: Se le pide responder a las preguntas de manera más objetiva posible, pues los datos que mencione son de gran valor e interés para el presente trabajo.

1. De acuerdo con su experiencia ¿Cuál es el impacto del delito informático en nuestra ciudad? Explique Ud.

Por el incremento del avance tecnológico los delitos informáticos se han visto incrementados de manera Acelerada.

2. De acuerdo con su experiencia ¿Considera que la conducta de la víctima contribuye a la perpetración del

delito informático? Explique Ud.

La falta de conocimiento en temas informáticos y la poca difusión de medidas preventivas genera vulnerabilidad en las victimas.

3. De acuerdo con su experiencia ¿Considera que la conducta de las entidades financieras en caso de fraude tarjetas de crédito contribuye a la perpetración del delito informático? Explique Ud.

Si, la falta de sistemas y mecanismos justificados contribuye a la comisión de delitos informáticos, aunado a la poca difusión preventiva de las entidades.

4. De acuerdo con su experiencia ¿Cuáles son las implicancias que conlleva falta de identificación de los partícipes del delito informático? Explique Ud.

La falta de mecanismos informáticos por parte de las entidades encargadas en la persecución de dichos delitos genera impunidad e impide sanciones a los avances directos de delitos informáticos.

5. En su opinión ¿Cuáles las medidas correctivas que deben adoptarse para hacer una persecución eficaz al delito informático? Explique Ud.

Adopción de mecanismos de lucha y sobre todo prevención en el ámbito de la informática.

LERY ROJAS HUANIO
Fiscal Adjunta Provincial
Primera Fiscalia Corporativa Especializada
en Ciberdelincuencia de Lima centro
Quinto Despacho Provincial

Firma del participante

Nombre: LERY ROJAS HUANIO

Fecha: 11.APR.2025

Universidad Nacional Federico Villarreal

Guía de entrevista

Título: "EFICACIA DE LA INVESTIGACIÓN FISCAL DE LOS DELITOS INFORMÁTICOS EN LAS FISCALÍAS ESPECIALIZADAS EN CIBERDELINCUENCIA DE LIMA CENTRO, 2024."

Entrevistadora: Malena Ayala Gonzales.

Profesión: Abogado

Grado académico: Magister.

Cargo: Tercer Despacho de la Primera Fiscalía Corporativa Especializada en Ciberdelincuencia de Lima Centro.

Institución donde labora: Ministerio Público.

Indicaciones: Se le pide responder a las preguntas de manera más objetiva posible, pues los datos que mencione son de gran valor e interés para el presente trabajo.

Preguntas:

1. De acuerdo con su experiencia ¿Cuál es el impacto del delito informático en nuestra ciudad? Explique Ud.

El impacto que ha traído consigo los delitos de informáticos – previsto en la Ley 30096 y sus modificaciones- es frenar el gran avance que se ha venido dando sobre la comisión de delitos bajo esta modalidad, busca hacer una lucha frontal y tener los mecanismos para no dejar impune esta nueva forma de delinquir, pues de no contar con tal normativa muchos actos que han generado gran perjuicio a las víctimas habrían quedado impunes.

2. De acuerdo con su experiencia ¿Considera que la conducta de la víctima contribuye a la perpetración del delito informático? Explique Ud.

No, debido a que existen múltiples modalidades que se vienen conociendo al hacer las investigaciones se aprecia que existe un déficit de seguridad en entidades bancarias y en algunas empresas, al haber una falta de implementación de programas que ciberseguridad, lo que termina poniendo en una situación de riesgo a la víctima (persona natural o jurídica); no obstante, si bien existe un porcentaje donde las víctimas de alguna manera facilitan algunos datos que contribuyen a la comisión de los delitos, este aspecto no puede ser atribuible a la misma pues ante la globalización que se viene afrontando no se puede exigir que las personas conozcan o tenga acceso a información respecto de la tecnología.

3. De acuerdo con su experiencia ¿Considera que la conducta de las entidades financieras en caso de fraude tarjetas de crédito contribuye a la perpetración del delito informático? Explique Ud.

Si, lamentablemente sus políticas de prevención de fraude que viene ostentando no son seguras ni resultan eficaz para combatir o frenar los casos de fraude con tarjetas de crédito, pues resulta muy fácil realizar operaciones con tan solo conocer las credenciales de acceso de las tarjetas de créditos, pese a que es de conocimiento público que en la actualidad existe un mercado negro donde se puede conseguir tal información. Por lo que, es de imperiosa necesidad que tales entidades mejoren sus políticas e implementen mayores planes de ciberseguridad.

4. De acuerdo con su experiencia ¿Cuáles son las implicancias que conlleva falta de identificación de los partícipes del delito informático? Explique Ud.

Debo comenzar indicando que al ser delitos informáticos una de las características de la misma es que el sujeto activo no es fácil de identificar, por tal motivo de no poder identificarse autores o coautores lamentablemente la investigación no será fructífera y deberá ser archivada pues conformé lo prevé el artículo 336 del CPP se debe "individualizar al sujeto activo"; sin embargo, cabe precisar que si se logra identificar al cómplice primario y/o secundario, pero no al autor o coautor, pero si se puede verificar la existencia del mismo dentro de los hechos, si resulta viable proseguir la causa.

Objetivo específico 2: Identificar las medidas correctivas deben adoptarse para hacer una persecución eficaz al delito informático

5. En su opinión ¿Cuáles las medidas correctivas que deben adoptarse para hacer una persecución eficaz al delito informático? Explique Ud.

El Estado debe exigir que las políticas de ciberseguridad de las entidades bancarias sean mejoradas, de igual forma respecto de los sistemas de las entidades públicos debe procurar que exista mejores niveles de control y seguridad – invertir también en planes se seguridad cibernética - para evitar que se realicen ataques a los mismos, como se ha venido dado últimamente; y ante el avance de nuevas modalidades de la comisión del delito informático haciendo uso de criptomonedas urge la creación de una billetera estatal para poder lograr la incautación de las mismas.

Firma del participante Nombre:
Malena Ayala Gonzales
Fecha:18/04/2025