Universidad Nacional José Faustino Sánchez Carrión

Escuela de Posgrado

Impunidad de los delitos informáticos y su afectación a los principios constitucionales en el Distrito Fiscal de Lima Centro, 2024

Tesis

Para optar el Grado Académico de Maestra en Derecho Constitucional y Administrativo

Autora

Elida Celeste Rojas Agurto

Asesor

Dr. Máximo Villarreal Salomé

Huacho – Perú

2026

UNIVERSIDAD NACIONAL
JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

LICENCIADA

(Resolución de Consejo Directivo N° 012-2020-SUNEDU/CD de fecha 27/01/2020

ESCUELA DE POSGRADO
MAESTRÍA EN DERECHO CONSTITUCIONAL Y ADMINISTRATIVO

METADATOS

DATOS DEL AUTOR (ES):		
APELLIDOS Y NOMBRES	**DNI**	**FECHA DE SUSTENTACIÓN**
Rojas Agurto, Elida Celeste	73543487	24-06-2026
DATOS DEL ASESOR:		
APELLIDOS Y NOMBRES	**DNI**	**CÓDIGO ORCID**
Villarreal Salomé, Máximo	40252721	https://orcid.org/0000-0003-1557-3138
DATOS DE LOS MIEMROS DE JURADOS – PREGRADO/POSGRADO-MAESTRÍA-DOCTORADO:		
APELLIDOS Y NOMBRES	**DNI**	**CODIGO ORCID**
Milán Matta, Bartolomé Eduardo	10536234	https://orcid.org/0000-0002-2256-8516
Aranda Bazalar, Nicanor Dario	15586303	https://orcid.org/0000-0001-8513-6676
Jiménez Fernández, Wilmer Magno	10136141	https://orcid.org/0000-0002-1776-7481

ELIDA CELESTE ROJAS AGURTO (2026-026734)

IMPUNIDAD DE LOS DELITOS INFORMÁTICOS Y SU AFECTACIÓN A LOS PRINCIPIOS CONSTITUCIONALES EN EL...

DGI-POSGRADO 2026

Dirección de Gestión de la Investigación-VRI 2026

DIRECCION DE GESTION DE LA INVESTIGACION

Detalles del documento

Identificador de la entrega
trn:oid:::1:3528921852

Fecha de entrega
6 abr 2026, 12:52 p.m. GMT-5

Fecha de descarga
6 abr 2026, 12:55 p.m. GMT-5

Nombre del archivo
TESIS_FINAL-ELIDA_ROJAS-MAESTRIA-TERMINADO.pdf

Tamaño del archivo
1.3 MB

106 páginas

23.309 palabras

144.924 caracteres

20% Similitud general

El total combinado de todas las coincidencias, incluidas las fuentes superpuestas, para ca...

Filtrado desde el informe

- Coincidencias menores (menos de 10 palabras)

Fuentes principales

19% Fuentes de Internet
5% Publicaciones
11% Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

Los algoritmos de nuestro sistema analizan un documento en profundidad para buscar inconsistencias que permitirían distinguirlo de una entrega normal. Si advertimos algo extraño, lo marcamos como una alerta para que pueda revisarlo.

Una marca de alerta no es necesariamente un indicador de problemas. Sin embargo, recomendamos que preste atención y la revise.

IMPUNIDAD DE LOS DELITOS INFORMÁTICOS Y SU AFECTACIÓN A LOS PRINCIPIOS CONSTITUCIONALES EN EL DISTRITO FISCAL DE LIMA CENTRO, 2024

ROJAS AGURTO, ELIDA CELESTE

TESIS DE MAESTRÍA

ASESOR: Dr. Máximo Villarreal Salomé

UNIVERSIDAD NACIONAL

JOSÉ FAUSTINO SÁNCHEZ CARRIÓN

ESCUELA DE POSGRADO

MAESTRA EN DERECHO CONSTITUCIONAL Y ADMINISTRATIVO

HUACHO

2026

DEDICATORIA

A mis padres Elida Agurto Ramírez y Alberto Rojas Alvarado, quienes, con su amor incondicional, su respaldo permanente y la fe depositada en mí, me enseñaron el valor de la constancia y me impulsaron a aspirar siempre a ser mejor.

A mis hermanos Isabel, Camila y Omar Rojas Agurto, quienes representan mi más grande fuente de inspiración; gracias por su paciencia, sus palabras de fortaleza y por acompañarme en cada momento de adversidad.

A mis abuelos Elpidio Agurto, Isabel Ramírez, Teodoro Rojas y Matilde Alvarado, quienes cultivaron en mí la convicción de que la educación es uno de los valores más trascendentales en la vida. Aunque su presencia física ya no está entre nosotros, su ejemplo permanece vivo en mí y sus bendiciones me guían ante cada nuevo reto.

A José P.R, mi compañero en este camino, cuyo soporte incondicional, optimismo y palabras de aliento fueron pilar fundamental en este proceso.

Este trabajo es para ustedes, mi querida familia, por confiar en mis capacidades y por constituir el soporte más sólido de mi existencia.

- *Abg. Rojas Agurto, Elida Celeste*

AGRADECIMIENTO

Expreso mi gratitud a Dios por acompañarme en cada etapa de mi vida, por concederme la fortaleza necesaria y la bendición de continuar desarrollándome en el ámbito profesional. A mi entrañable familia, quien ha constituido mi sostén incondicional a lo largo de todos estos años, manteniéndose presente en cada etapa de este recorrido. Su cariño y sus palabras de motivación han sido piezas fundamentales para poder alcanzar este tan esperado logro.

- *Abg. Rojas Agurto Elida Celeste*

ÍNDICE

Índice de tablas

Índice de figuras

Resumen

Introducción: La presente investigación se titula: Impunidad de los delitos informáticos y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024, considerando como **Problema General**: ¿Qué relación tiene la impunidad de los delitos informáticos y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024? A partir de ello, se plantea como posible respuesta que la impunidad de los delitos informáticos se relaciona significativamente con su afectación a los Principios constitucionales del Distrito Fiscal de Lima Centro, 2024. **Metodología:** Se plantea una investigación de tipo básica, nivel descriptivo-correlacional, enfoque mixto y diseño no experimental. Asimismo, se consideró como población de estudio a 180 operadores jurídicos del Distrito Fiscal de Lima Centro, obteniéndose una muestra de 63 operadores jurídicos mediante muestreo probabilístico, con una confiabilidad de 0.842. **Conclusión:** Existe una relación estadísticamente significativa ($r=0.817$, $p<0.01$) entre la impunidad de los delitos informáticos y la afectación a los principios constitucionales en el Distrito Fiscal de Lima Centro, 2024. La deficiente especialización de los operadores jurídicos, la carencia de recursos tecnológicos y la ausencia de protocolos especializados generan archivos fiscales que vulneran sistemáticamente garantías constitucionales fundamentales. **Recomendación:** Es fundamental que el Ministerio Público, en colaboración con el Poder Judicial y el Ministerio de Justicia y Derechos Humanos, impulse la creación de fiscalías y juzgados especializados en delitos informáticos, implemente programas de capacitación técnica obligatoria para operadores jurídicos, y establezca protocolos estandarizados de investigación forense digital que garanticen la tutela jurisdiccional efectiva en el ámbito cibernético.

Palabras clave: Delitos informáticos, impunidad, principios constitucionales, tutela jurisdiccional efectiva, debido proceso, fraude informático, sabotaje informático, acceso ilícito.

Abstract

Introduction: The present research is entitled: Impunity of computer crimes and its impact on Constitutional Principles in the Central Lima Fiscal District, 2024, considering as General **Problem**: What relationship exists between the impunity of computer crimes and its impact on Constitutional Principles in the Central Lima Fiscal District, 2024? From this, it is proposed as a possible answer that the impunity of computer crimes is significantly related to its impact on the Constitutional Principles of the Central Lima Fiscal District, 2024. **Methodology:** A basic type of research is proposed, descriptive-correlational level, mixt approach, and non-experimental design. Likewise, the study population was considered to be 180 legal operators from the Fiscal District of Lima Centro, obtaining a sample of 63 legal operators through probabilistic sampling, with a reliability of 0.842. **Conclusion:** There is a statistically significant relationship ($r=0.817$, $p<0.01$) between the impunity of cybercrimes and the impact on constitutional principles in the Fiscal District of Lima Centro, 2024. The deficient specialization of legal operators, the lack of technological resources, and the absence of specialized protocols generate fiscal archives that systematically violate fundamental constitutional guarantees. **Recommendation:** It is essential that the Public Prosecutor's Office, in collaboration with the Judiciary and the Ministry of Justice and Human Rights, promote the creation of specialized prosecutor's offices and courts for computer crimes, implement mandatory technical training programs for legal operators, and establish standardized digital forensic investigation protocols that guarantee effective jurisdictional protection in the cyber sphere.

Keywords: Computer crimes, impunity, constitutional principles, effective jurisdictional protection, due process, computer fraud, computer sabotage, illicit access.

Introducción

El presente trabajo de investigación surge de la necesidad de examinar una realidad que viene afectando de manera silenciosa pero profunda la administración de justicia en el Perú: la incapacidad del sistema judicial para responder de forma efectiva ante la criminalidad que se desarrolla en entornos digitales. Si bien el ordenamiento jurídico peruano reconoce formalmente los delitos informáticos a través de la Ley N.° 30096, esta regulación no ha logrado traducirse en una persecución penal eficiente en la práctica, lo que ha derivado en una preocupante situación de impunidad que, a su vez, repercute negativamente sobre garantías de rango constitucional.

El Distrito Fiscal de Lima Centro constituyó el escenario de análisis de esta investigación, por concentrar una importante actividad jurisdiccional en materia penal y representar un espacio relevante para examinar cómo los operadores jurídicos enfrentan o dejan de enfrentar los desafíos que plantea la criminalidad cibernética. Las dificultades identificadas en este contexto van desde la escasa preparación técnica de fiscales y magistrados hasta los problemas asociados a la recolección y conservación de evidencia digital, pasando por la ausencia de mecanismos institucionales suficientemente especializados para abordar este tipo de ilícitos.

Desde una perspectiva constitucional, esta problemática no es menor. La impunidad en delitos como el fraude informático, el sabotaje de sistemas y el acceso ilícito a datos privados no solo representa una falla en la respuesta punitiva del Estado, sino que compromete derechos fundamentales de las víctimas que merecen protección efectiva: el derecho a la intimidad, la reserva de los datos personales, la tutela jurisdiccional efectiva,

el debido proceso y la seguridad jurídica. Cuando el sistema de justicia no logra identificar, procesar y sancionar a los responsables de estas conductas, los afectados quedan en un estado de desamparo que el Estado constitucional de derecho no puede tolerar.

Frente a esta realidad, la investigación se propuso no solo diagnosticar el problema, sino también contribuir a su solución. Para ello, se examinaron los fundamentos doctrinarios, normativos y constitucionales que subyacen a esta problemática, con el propósito de identificar con precisión qué factores propician la impunidad y qué reformas o medidas serían necesarias para revertirla. En particular, se prestó atención a la necesidad de fortalecer las capacidades técnicas de los operadores del sistema judicial, mejorar los procedimientos de investigación forense en entornos digitales y consolidar instancias especializadas que permitan dar una respuesta penal proporcional, oportuna y constitucionalmente coherente ante la ciberdelincuencia.

Se espera que los hallazgos de este estudio aporten elementos concretos para la mejora del sistema de justicia penal peruano en este ámbito, contribuyendo a que las víctimas de delitos informáticos cuenten con una protección jurisdiccional real y que la impunidad deje de ser la regla en un escenario donde la tecnología avanza más rápido que la respuesta institucional del Estado.

Capítulo I: Planteamiento del problema

1.1. Descripción de la realidad problemática

Hoy en día, la criminalidad que se desarrolla a través de medios tecnológicos representa uno de los fenómenos delictivos más difíciles de abordar dentro del derecho penal moderno. Su complejidad radica en que las tecnologías de la información y la comunicación no solo facilitan la comisión de estos ilícitos, sino que en muchos casos constituyen el objeto mismo sobre el que recae la conducta punible. Villavicencio Terreros (2014) advierte que esta forma de delinquir, a la que denomina "delitos informativos", es una consecuencia directa del vertiginoso avance de las herramientas informáticas, lo que exige a quienes la estudian y persiguen un dominio simultáneo de los aspectos técnicos y de los fundamentos jurídicos que la regulan. En el caso peruano, esta realidad ha cobrado una dimensión particularmente preocupante en los últimos años, pues el incremento sostenido de estas conductas ha puesto en evidencia las limitaciones de las categorías tradicionales del derecho penal y constitucional para dar respuesta adecuada a un fenómeno que no cesa de evolucionar (García Toma, 2003).

La impunidad en los delitos informáticos se refiere a la ausencia de sanción penal efectiva para quienes cometen estos ilícitos, generando un estado de desprotección para las víctimas y un mensaje de tolerancia hacia la criminalidad cibernética. Según la doctrina penal especializada, esta problemática se manifiesta a través de diversos factores estructurales del sistema penal, siendo uno de los principales la dificultad para la individualización del ciberdelincuente, lo que conduce frecuentemente al archivo de los procesos penales por parte del Ministerio Público debido a la imposibilidad de formalizar la investigación preparatoria contra personas identificadas (Villavicencio Terreros, 2014). Esta problemática no solo afecta la eficacia del sistema penal, sino que también compromete gravemente los principios

constitucionales fundamentales que sustentan el Estado de Derecho (Landa Arroyo, 2012).

El derecho penal y el derecho administrativo no operan en un vacío normativo. Su funcionamiento está orientado y limitado por un conjunto de principios que la Constitución reconoce como indisponibles, y que cumplen una función doble: por un lado, garantizan que la administración de justicia se desarrolle de manera correcta y predecible; por otro, protegen a los ciudadanos frente al ejercicio desmedido o arbitrario del poder estatal. García Toma (2003) los caracteriza como mandatos de optimización, es decir, directrices que no se aplican de manera rígida, sino que orientan la interpretación constitucional y actúan como freno ante cualquier exceso del ius puniendi. Sin ellos, el Estado de Derecho perdería su sustento más profundo.

Entre los principios que mayor relevancia cobran en este contexto se encuentran el debido proceso, el acceso efectivo a la justicia, la tutela jurisdiccional efectiva, la igualdad de trato ante la ley y el principio de legalidad. Cada uno de ellos representa una garantía concreta para las personas que acuden al sistema de justicia esperando una respuesta justa y oportuna. El problema surge cuando esa respuesta no llega. Cuando los delitos informáticos quedan sin sanción, no es solo el agresor quien sale impune: son también estos principios los que resultan vulnerados, uno a uno, de manera acumulativa. Y esa vulneración sistemática no tarda en traducirse en algo más profundo y difícil de revertir: la pérdida de confianza de los ciudadanos en las instituciones que, en teoría, existen para protegerlos (Bernales Ballesteros, 2012).

En el ámbito nacional, la situación que enfrenta el Perú en torno a la falta de sanción efectiva de los delitos cometidos en entornos digitales responde a una serie de factores de orden estructural y normativo que se han ido acumulando con el tiempo. Si bien la promulgación de

la Ley N.° 30096 en el año 2013 supuso un avance importante al dotar al sistema jurídico de un marco específico para prevenir y castigar las conductas que atentan contra los sistemas y datos informáticos, lo cierto es que su implementación en la práctica ha revelado carencias notorias que terminan favoreciendo la impunidad. Al respecto, Peña Cabrera (2015) pone de relieve que la correcta aplicación de estos tipos penales demanda una lectura integral que no se limite a los elementos clásicos de la teoría del delito, sino que incorpore también el entendimiento de las particularidades técnicas propias de los medios informáticos involucrados. Esta exigencia genera, inevitablemente, dificultades adicionales tanto en la fase de investigación como en el momento del juzgamiento, dificultades que el sistema de justicia peruano aún no ha logrado superar de manera satisfactoria.

El Distrito Fiscal de Lima Centro, como una de las jurisdicciones con mayor incidencia de delitos informáticos debido a su concentración poblacional y actividad comercial, representa un escenario crítico para el análisis de esta problemática. En esta jurisdicción confluyen múltiples factores que exacerban la impunidad: alta incidencia delictiva, limitaciones tecnológicas de los operadores de justicia, insuficiente especialización del personal fiscal y judicial, y deficiencias en los protocolos de investigación de delitos cibernéticos. Estas circunstancias generan un escenario donde la vulneración de los principios constitucionales se hace más evidente y sistemática, afectando particularmente el derecho a la tutela jurisdiccional efectiva y el debido proceso (Huerta Guerrero, 2018).

Analizar la impunidad en materia de delitos informáticos desde el derecho constitucional y administrativo permite advertir que sus consecuencias van mucho más allá de lo que ocurre en un caso concreto. No se trata únicamente de que una víctima quede sin justicia; se trata de un problema que, cuando se repite, afecta la seguridad jurídica de todos y debilita

la confianza que la sociedad deposita en sus instituciones. Landa Arroyo (2014) nos recuerda que el proceso de constitucionalización del derecho administrativo ha traído consigo una consecuencia de enorme calado: ya no es posible concebir ningún acto de la administración pública, incluida la función jurisdiccional del Estado, como ajeno a los principios constitucionales. Todo lo que el Estado hace o deja de hacer debe poder medirse con ese rasero. Y cuando la persecución penal falla, cuando los responsables de delitos informáticos no son investigados ni sancionados, esa omisión no es un simple problema de gestión: es una vulneración concreta de los derechos fundamentales que el propio Estado tiene el deber ineludible de proteger.

En el derecho comparado, diversos países han adoptado enfoques diferenciados para abordar la criminalidad informática y garantizar el respeto a los principios constitucionales. Por ejemplo, España ha desarrollado unidades especializadas de investigación y protocolos específicos para delitos cibernéticos, implementando además reformas procesales que facilitan la obtención de evidencia digital. Colombia, por su parte, ha fortalecido su marco normativo con reformas que facilitan la investigación y persecución de estos ilícitos, incorporando herramientas de cooperación internacional y fortalecimiento de capacidades técnicas. Estas experiencias evidencian la necesidad de reformas integrales que no solo fortalezcan el marco normativo, sino que también mejoren las capacidades operativas del sistema de justicia penal.

La afectación a los principios constitucionales derivada de la impunidad en delitos informáticos se manifiesta de múltiples formas en el ordenamiento jurídico peruano. El derecho al debido proceso se ve comprometido cuando las investigaciones no se realizan con la diligencia debida o cuando se archivan prematuramente por falta de especialización técnica de los operadores de justicia. El acceso a la justicia se vulnera cuando las víctimas no

encuentran respuestas efectivas del sistema judicial, generando una sensación de desamparo institucional. La tutela jurisdiccional efectiva se afecta cuando no existe una protección real y concreta de los derechos vulnerados por los delitos informáticos, contraviniendo lo establecido en el artículo 139° inciso 3 de la Constitución Política del Perú (García Belaunde, 2016).

Adicionalmente, la problemática se agrava cuando consideramos que los delitos informáticos, por su naturaleza transnacional y la utilización de medios tecnológicos sofisticados, requieren de respuestas especializadas que el sistema de justicia peruano aún no ha desarrollado plenamente. Esta deficiencia no solo genera impunidad, sino que también crea incentivos perversos para la proliferación de estas conductas delictivas, afectando así el principio constitucional de seguridad jurídica y el deber del Estado de garantizar la seguridad de las personas (Quiroga León, 2014).

En definitiva, el presente trabajo busca aproximarse de manera exhaustiva a una problemática que viene afectando de forma silenciosa pero persistente el funcionamiento del sistema de justicia penal en el Perú: la incapacidad para sancionar de manera efectiva los delitos que se cometen a través de medios digitales y las consecuencias que ello trae sobre garantías de rango constitucional, todo ello examinado desde la experiencia concreta del Distrito Fiscal de Lima Centro a lo largo del año 2024. Para alcanzar ese propósito, el estudio se orienta en tres direcciones complementarias: determinar qué elementos están detrás de esta falta de respuesta punitiva, medir el nivel en que los principios constitucionales esenciales se ven comprometidos desde la óptica del derecho constitucional y administrativo, y formular propuestas concretas que permitan dotar al sistema de justicia penal de mejores herramientas para perseguir con eficacia la criminalidad informática.

Más allá de los hallazgos técnicos o normativos que puedan derivarse del análisis, lo que en el fondo persigue esta investigación es contribuir a que el Estado de Derecho no quede rezagado frente al avance tecnológico, y a que los ciudadanos cuenten con una protección real y efectiva de sus derechos fundamentales cuando estos son vulnerados en entornos digitales. Un sistema de justicia que no logra adaptarse a los retos que impone la era digital termina siendo un sistema que defrauda a quienes más lo necesitan, y es precisamente esa brecha la que este trabajo aspira a contribuir a cerrar, siempre dentro del marco de los principios y valores que inspiran nuestro ordenamiento constitucional.

1.2. Formulación del problema

1.2.1. Problema general

¿Qué relación tiene la impunidad de los delitos informáticos y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024?

1.2.2. Problemas específicos

Pe1: ¿Qué relación existe entre el fraude informático y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024?

Pe2: ¿Qué relación existe entre el sabotaje informático y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024?

Pe3: ¿Qué relación existe entre el acceso ilícito y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024?

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Determinar la relación que existe entre la impunidad de los delitos informáticos y su

afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024.

1.3.2. Objetivos Específicos

Oe1: Determinar la relación que existe entre el fraude informático y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024

Oe2: Determinar la relación que existe entre el sabotaje informático y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024

Oe3: Determinar la relación que existe entre el acceso ilícito y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024

1.4. Justificación de la investigación

1.4.1. Justificación teórica

Uno de los aspectos que justifica la realización de este trabajo desde el plano teórico es la ausencia de un desarrollo doctrinario suficientemente articulado que permita entender, con la profundidad que merece, de qué manera la falta de sanción efectiva en materia de criminalidad informática termina erosionando principios que el ordenamiento constitucional peruano reconoce como pilares del sistema jurídico. La protección genuina de los derechos fundamentales no puede reducirse a su consagración formal en el texto constitucional; requiere, además, que los mecanismos de tutela jurisdiccional funcionen de manera real, que el acceso a la justicia no sea una promesa vacía y que las garantías del debido proceso operen en la práctica. Cuando la persecución penal de los delitos informáticos fracasa sistemáticamente, todos esos principios quedan comprometidos de una forma que pocas veces ha sido examinada con rigor (García Toma, 2003).

A ello se suma que la aplicación deficiente de la normativa penal especializada en este ámbito no solo genera espacios de desprotección para las víctimas, sino que produce tensiones

concretas en el funcionamiento del sistema de justicia, derivando en decisiones jurisdiccionales que no alcanzan los estándares constitucionales exigibles. Frente a esa realidad, la presente investigación aspira a construir un conjunto de criterios teóricos que sirvan de referencia para los operadores jurídicos, dotándolos de una base conceptual sólida desde la cual comprender la dimensión constitucional del problema y orientar su actuación hacia una protección de los derechos fundamentales que sea verdaderamente efectiva y coherente con los mandatos que emanan de la Constitución (Landa Arroyo, 2014).

1.4.2. Justificación metodológica

La elección del enfoque metodológico en una investigación no es una decisión menor; responde a la naturaleza del problema que se estudia y a los objetivos que se persiguen. En el caso del presente trabajo, el enfoque mixto resulta el más adecuado. Si bien la problemática involucra percepciones, experiencias y valoraciones de quienes operan cotidianamente dentro del sistema de justicia, este enfoque permite sistematizar, medir y procesar objetivamente dichas apreciaciones a través de herramientas estadísticas comprobables. Desde esa mirada, el estudio busca medir y evidenciar de qué manera la falta de respuesta punitiva efectiva frente a la criminalidad informática repercute sobre los principios que la Constitución reconoce como fundamentales para el ejercicio de la justicia, examinando esta realidad tal como se manifiesta en el Distrito Fiscal de Lima Centro durante el año 2024. Este enfoque permite ir más allá de la superficie normativa, recogiendo de forma estructurada las voces de los profesionales del derecho que lidian con esta problemática en su quehacer diario, para traducirlas en datos fiables que sustenten la magnitud del fenómeno.

Del mismo modo, se adoptará un nivel de investigación de carácter descriptivo-correlacional, dado que se pretende establecer el grado de vinculación y asociación estadísticamente significativa entre las variables, determinando de qué forma la ausencia de responsabilidad penal en delitos de índole informática se relaciona directamente con la vulneración a los principios constitucionales. Al tratarse de un diseño no experimental, no se busca aislar variables bajo una estricta lógica de laboratorio (causa y efecto puro), sino medir cómo interactúan en su contexto real. Adicionalmente, si bien la investigación es de tipo básica, esta no se limitará a un análisis abstracto, sino que abordará la realidad del sistema de administración de justicia en el Perú. El propósito es generar un marco de comprensión teórico-doctrinario que sirva de base para futuras alternativas de solución jurídico-constitucionales, contribuyendo así al afianzamiento del Estado de Derecho.

1.4.3. Justificación social

El fundamento social de la presente investigación se asienta en la urgencia de garantizar la plena vigencia de los derechos fundamentales y consolidar la credibilidad de la ciudadanía frente al sistema de justicia penal peruano, en el marco del contexto digitalizado actual. En toda sociedad que se rige bajo principios democráticos y constitucionales, resulta indispensable que las resoluciones judiciales respondan a criterios de equidad, proporcionalidad y tutela efectiva, de modo que quienes incurran en conductas delictivas de naturaleza informática sean debidamente investigados y sancionados, y que las personas afectadas cuenten con una protección jurisdiccional real y eficaz.

La continuidad de la impunidad en este tipo de delitos genera en la sociedad una sensación de desamparo y una creciente desconfianza hacia las instituciones estatales, erosionando la legitimidad del aparato judicial y afectando la cohesión colectiva en un contexto

donde la tecnología digital se ha convertido en un componente inseparable de la vida cotidiana. Al examinar esta problemática y proponer lineamientos orientados a asegurar la vigencia efectiva de los principios constitucionales frente a la criminalidad informática, el presente estudio aspira a robustecer la credibilidad del sistema de justicia, impulsar la seguridad jurídica en el entorno digital y aportar a la edificación de una sociedad con mayor protección constitucional.

Por otro lado, al poner en diálogo el análisis de esta problemática con los parámetros que tanto la Constitución como los instrumentos internacionales establecen para la protección de derechos en entornos digitales, este trabajo aporta elementos concretos para consolidar el Estado Constitucional de Derecho y para que el Perú honre los compromisos que ha asumido ante la comunidad internacional en materia de garantías fundamentales dentro de la sociedad tecnológica actual.

En el fondo, lo que esta investigación aspira a lograr tiene una dimensión muy concreta: que los ciudadanos peruanos cuenten con una protección jurisdiccional que funcione de verdad. No una protección que existe solo en los textos legales o en las declaraciones institucionales, sino una que se materialice en decisiones judiciales justas, en normas que se aplican con coherencia y en garantías que las personas puedan invocar con la certeza de que serán respetadas. En un contexto donde la vida cotidiana transcurre cada vez más en entornos digitales, esa protección ya no puede pensarse al margen de la realidad tecnológica. Quienes hoy trabajan, se comunican y construyen su identidad a través de medios digitales merecen que el sistema de justicia esté a la altura de los riesgos que eso conlleva. Contribuir a que esa brecha se cierre es, en última instancia, la razón de ser de este trabajo.

1.5. Delimitación del estudio

1.5.1. Delimitación temática: La presente investigación se inscribe en el ámbito del Derecho, con énfasis particular en las ramas del Derecho Constitucional y el Derecho Administrativo, centrándose en el resguardo de los principios constitucionales frente al fenómeno de los delitos informáticos y su repercusión en el funcionamiento del sistema de justicia.

1.5.2. Delimitación espacial: El estudio tendrá como escenario el Distrito Fiscal de Lima Centro, perteneciente al Distrito Judicial de Lima, ubicado en el departamento de Lima, en la República del Perú.

1.5.3. Delimitación poblacional: Conforme a los criterios muestrales establecidos, los sujetos participantes en esta investigación serán fiscales y jueces de la especialidad penal, defensores públicos, así como abogados con formación especializada en derecho penal y constitucional que desempeñan su labor profesional vinculada al ámbito del Distrito Fiscal de Lima Centro.

Capítulo II: marco teórico

2.1. Antecedentes de la investigación

2.1.1. Antecedentes internacionales

Velasco San Martín, Cristos (2011) desarrolló una investigación de nivel doctoral titulada "El derecho y la jurisdicción aplicable en materia de conductas delictivas cometidas en internet a la luz del convenio sobre ciberdelincuencia del Consejo de Europa con un particular enfoque en México y países de Latinoamérica", el trabajo fue defendido en la Universidad Carlos III de Madrid, España, como parte de los requisitos exigidos para alcanzar el grado de Doctor en Derecho. Metodológicamente, el autor se valió de una perspectiva dogmático-jurídica inscrita dentro de la modalidad de investigación teórica aplicada, con un nivel de análisis descriptivo-explicativo y un diseño comparativo que permitió contrastar distintos ordenamientos jurídicos. La revisión y el análisis de fuentes documentales y jurisprudenciales constituyeron los principales instrumentos de los que se sirvió el investigador para construir su argumentación, lo que le permitió formular las siguientes conclusiones:

> La jurisdicción aplicable en delitos cometidos en el ciberespacio presenta desafíos únicos que requieren una reinterpretación de los principios constitucionales tradicionales de soberanía y territorialidad. La impunidad resultante de las lagunas jurisdiccionales y normativas constituye una violación sistemática del derecho a la tutela judicial efectiva, demandando respuestas integrales que armonicen la cooperación internacional con la protección de los derechos fundamentales en el entorno digital. El análisis comparativo evidencia que la efectividad de la persecución de delitos informáticos depende directamente del fortalecimiento de las garantías constitucionales procesales y

la especialización de los operadores de justicia. (p. 456)

Morales Sánchez, Diego Alejandro (2023) llevó a cabo un estudio denominado "Delitos Informáticos", presentado ante la Universidad Libre de Colombia como requisito para alcanzar el Grado Académico de Magíster en Derecho Penal. La investigación se desenvolvió bajo una perspectiva metodológica de naturaleza cuantitativa y cualitativa, con un tipo de investigación aplicada, alcance explicativo y diseño fenomenológico. Los instrumentos de recolección de información empleados incluyeron entrevistas de carácter estructurado, revisión y análisis de fuentes documentales, así como el examen de estadísticas de orden judicial, elementos que en conjunto permitieron formular las siguientes conclusiones:

> La evaluación de la eficacia de la Ley 1273 de 2009 de Delitos Informáticos en Colombia revela serias deficiencias en su aplicación práctica que comprometen la efectividad de los principios constitucionales del debido proceso y la tutela judicial efectiva. Los hallazgos evidencian que la impunidad en delitos cibernéticos alcanza niveles superiores al 85%, generando una crisis de confianza ciudadana en el sistema de justicia y una afectación sistemática a los derechos fundamentales. La falta de especialización de los operadores judiciales, la insuficiencia de recursos tecnológicos y las limitaciones en la cooperación internacional constituyen los principales factores que perpetúan esta problemática, demandando reformas estructurales urgentes que garanticen una protección efectiva de los derechos constitucionales en el entorno digital. (p. 289)

Astrith Iliana Cuenca Gonzaga y Juri Evelyn Núñez Portilla (2024) en su artículo orientado al análisis documental sobre la incidencia de la seguridad jurídica frente a la criminalidad

informática, retoman el pensamiento de Monereo Pérez (2022), quien alude a Hans Kelsen ,uno de los juristas más trascendentales de la teoría del derecho, para señalar que la seguridad jurídica constituye un principio inherente al ordenamiento normativo que asegura la posibilidad de anticipar las consecuencias del derecho. Dicha seguridad se alcanza cuando las disposiciones normativas reúnen las condiciones de claridad, precisión y estabilidad, otorgando a los ciudadanos la capacidad de prever los efectos jurídicos derivados de su conducta. En ese sentido, la seguridad jurídica resulta indispensable para la validez del derecho positivo, toda vez que garantiza una aplicación uniforme y exenta de arbitrariedad.

Por su parte, Julio Téllez Valdés, jurista de amplia trayectoria en el ámbito del derecho tecnológico, las conductas delictivas de naturaleza informática pueden entenderse como aquellos actos contrarios a la ley que se ejecutan valiéndose de recursos propios de las tecnologías de la información y la comunicación, ocasionando con ello una afectación a atributos esenciales como la reserva, la exactitud y la accesibilidad de los datos e infraestructuras digitales. El referido autor subraya que el espectro de estas conductas es considerablemente amplio, pues no se circunscribe únicamente a la intrusión no autorizada en sistemas, sino que engloba igualmente actuaciones como el engaño económico a través de medios digitales, la usurpación de la identidad ajena y la diseminación de software de naturaleza maliciosa (Ormaza & Ycaza, 2023).

En cuanto a los ataques informáticos, estos son entendidos como acciones de naturaleza maliciosa dirigidas contra sistemas, redes o dispositivos tecnológicos, con el propósito de ocasionar perjuicios, sustraer información, vulnerar accesos o interrumpir la operatividad habitual de los servicios. Estas amenazas representan un riesgo considerable para la integridad y la seguridad de los sistemas en el entorno digital. El conocimiento de sus diversas manifestaciones resulta clave para diseñar estrategias de protección eficientes y salvaguardar los activos informacionales. Tanto organizaciones como individuos deben mantenerse permanentemente actualizados e implementar

medidas de seguridad sólidas para hacer frente a este tipo de amenazas (Ribera et al., 2022).

Stallings William (2017) en su obra *Cryptography and Network Security: Principles and Practice*, entiende los ataques informáticos como actuaciones intencionales cuya finalidad es quebrantar la integridad de la información y el funcionamiento de los sistemas de comunicación. El autor establece una distinción entre dos categorías fundamentales: por un lado, los ataques de naturaleza pasiva, caracterizados por la captación subrepticia de datos sin intervención directa sobre ellos; y por otro, los ataques de carácter activo, que implican una manipulación efectiva de la información o una interferencia deliberada sobre la operatividad de los sistemas.

Tipos y Modalidades de Delitos Informáticos

- Acceso no Autorizado (Hacking)
- Intercepción de Comunicaciones (Sniffing)
- Daños o Alteración de Datos (Data Diddling)
- Fraude Informático
- Phishing
- Distribución de Malware
- Robo de Identidad
- Modalidades de Delitos Informáticos
- Ciberterrorismo
- Ciberespionaje
- Ciberacoso
- Fraude Electrónico
- Sabotaje Informático
- Estafas en Línea

Como resultado de su análisis, los autores sostienen que Ecuador ha experimentado avances

notorios en la consolidación de su arquitectura jurídica e institucional orientada a enfrentar la criminalidad en entornos digitales, si bien continúan presentándose retos propios de un ecosistema tecnológico en constante evolución. En cuanto al plano normativo, el país cuenta con disposiciones legales concretas que sancionan una variedad de conductas ilícitas vinculadas a este fenómeno, entre las que figuran la intrusión no autorizada en sistemas, las acciones de sabotaje digital y el engaño económico a través de medios informáticos. En ese marco, la Ley Orgánica de Comunicación incorpora preceptos destinados a resguardar la información de carácter personal y a establecer responsabilidades frente a su divulgación indebida.

De manera complementaria, el ordenamiento ecuatoriano contempla normativas específicas en materia de datos personales, cuya supervisión recae en organismos como la Agencia de Regulación y Control de las Telecomunicaciones (ARCOTEL) y la Superintendencia de Información y Comunicación (SUPERCOM), entidades encargadas de velar porque tanto el sector público como el privado adopten prácticas adecuadas en el tratamiento de la información ciudadana. Paralelamente, se vienen impulsando programas de educación y concientización en torno a la seguridad digital, dirigidos a distintos sectores de la sociedad, incluyendo la ciudadanía en general, el mundo empresarial y los funcionarios del Estado, con el propósito de reducir la ocurrencia de incidentes cibernéticos y elevar la capacidad institucional de respuesta. En última instancia, la edificación de un sistema normativo sólido resulta determinante para sostener la confianza colectiva en las herramientas digitales, siendo la apropiación de una cultura de seguridad en línea un pilar indispensable para el desarrollo continuo de la innovación tecnológica.

2.1.2 Antecedentes nacionales

Urdanegui Rangel, Anabeliza (2023) mediante su proyecto de investigación denominado: "Los delitos informáticos y la vulneración del derecho fundamental de protección

de datos personales en Lima Metropolitana", presentado ante la Universidad Autónoma del Perú para la obtención del Título de Abogado; para ello, el investigador utilizó el tipo de investigación básica, diseño correlacional, nivel descriptivo-explicativo y enfoque cuantitativo, empleando como instrumentos encuestas y análisis documental, llegando a la siguiente conclusión:

> A criterio del autor, la respuesta más adecuada frente a la problemática que plantea la criminalidad informática reside en la formulación, por parte del Estado, de una Política Nacional de Ciberseguridad que articule un conjunto integral de medidas preventivas orientadas a reducir la exposición de los ciudadanos ante este tipo de conductas delictivas. En esa línea, señala que los ilícitos cometidos en entornos digitales ocasionan una lesión directa al derecho fundamental a la protección de la información personal, poniendo al descubierto fallas estructurales dentro del sistema de justicia penal que debilitan la vigencia real de principios constitucionales como la seguridad jurídica y la tutela judicial efectiva. A ello se suma que la falta de sanción derivada de dichas deficiencias produce un efecto expansivo que va minando progresivamente la credibilidad de los ciudadanos en las instituciones que sostienen el orden democrático. (p. 89).

Torres Cáceres, María Elena (2024) a través de su investigación denominada: "La ciberdelincuencia y los delitos informáticos con mayor incidencia en el Perú 2024", presentado ante la Universidad César Vallejo como requisito para obtener el Grado Académico de Maestro en Gestión Pública. La investigación se desarrolló bajo una perspectiva cualitativa, con un tipo de investigación básica, alcance descriptivo y diseño no experimental. Para la recolección y

tratamiento de la información se recurrió al análisis documental y a fuentes de carácter secundario, lo que permitió arribar a las siguientes conclusiones:

> Los delitos informáticos con mayor incidencia en el Perú corresponden principalmente a delitos contra el patrimonio y contra la fe pública, evidenciando una problemática creciente que requiere respuestas integrales del Estado. La falta de especialización y la deficiente aplicación del marco normativo contribuyen a generar impunidad, afectando los principios constitucionales de seguridad jurídica y protección efectiva de los derechos fundamentales. El análisis evidencia que la impunidad alcanza niveles superiores al 90% en este tipo de delitos, constituyendo una vulneración sistemática del derecho a la tutela judicial efectiva y generando un grave impacto en la confianza ciudadana hacia el sistema de justicia peruano. (p. 134).

Guevara Azula, Anamin Consuelo (2024) desarrolló un proyecto de investigación denominado "Evaluación del delito informático en agravio de los ciudadanos en Huancayo, 2024", el cual fue presentado ante la Universidad César Vallejo como requisito para alcanzar el Grado Académico de Maestro en Derecho Penal y Procesal Penal. La investigadora orientó su estudio bajo un tipo de investigación aplicada, con un diseño de carácter no experimental, alcance descriptivo-correlacional y perspectiva metodológica cualitativa. Como instrumentos de recolección de información se emplearon cuestionarios estructurados aplicados a fiscales y asistentes fiscales, lo que permitió arribar a la siguiente conclusión:

> La evaluación de los delitos informáticos en agravio de los ciudadanos evidencia una problemática creciente que requiere una respuesta integral del sistema de justicia. Las deficiencias en la investigación y persecución de estos

> delitos generan impunidad y afectan directamente los principios constitucionales del debido proceso y la tutela jurisdiccional efectiva, demandando reformas que fortalezcan la protección de los derechos fundamentales en el ámbito digital. Los resultados del estudio revelan que el 78% de los casos de delitos informáticos no llegan a tener una resolución satisfactoria, evidenciando graves falencias en la aplicación de los principios constitucionales de eficacia y celeridad procesal. (p. 189)

Catalina Tania Estrada Salvador Ramírez (2024) investigadora adscrita a la Universidad de Huánuco, Perú, publicó un artículo científico titulado "La impunidad en los delitos informáticos. Una problemática de poco interés para legisladores, jueces y fiscales", difundido en la revista académica Ius Vocatio, órgano de investigación de la Corte Superior de Justicia de Huánuco, correspondiente al volumen 7, número 9, del período enero-junio de 2024, páginas 91 a 115, con periodicidad semestral, ISSN: 2810-8043 (versión en línea) y DOI: 10.35292/iusVocatio.v7i9.928. En el apartado de recomendaciones de dicho trabajo, la autora propone un conjunto de alternativas orientadas a dar solución a la problemática de la impunidad en materia de delitos informáticos, señalando lo siguiente:

> 1. **Creación de herramientas tecnológicas** Es importante destacar que, en el marco del 12.° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, se examinaron diversos mecanismos y recursos de carácter legal que revisten especial relevancia. En ese contexto, se puso de manifiesto la necesidad de contar con instrumentos normativos adecuados, dado que la eficacia en la aplicación de la ley está estrechamente vinculada a la disponibilidad de medios de investigación especializados, entre los cuales

destacan los programas de informática forense orientados a la recolección de evidencias, el registro de actividad en dispositivos y la recuperación de archivos borrados. De igual manera, resulta indispensable disponer de sistemas informáticos y repositorios de datos para la gestión de investigaciones, incorporando funcionalidades como el sistema de «hash» aplicado a imágenes de explotación sexual infantil (Espinoza Calderón, 2022, p. 58).

El avance en el desarrollo de herramientas tecnológicas para la investigación forense digital ha sido notable en los últimos tiempos. Un ejemplo representativo es el proyecto «Reconstrucción Automática de Eventos para el Análisis Forense Digital y de Intrusiones», gestado en el University College de Dublín, cuyo propósito es automatizar la reconstrucción de incidentes digitales con fines investigativos. En esa misma dirección, los Estados Unidos pusieron en marcha la tecnología Photo DNA, una herramienta concebida específicamente para identificar y seguir el rastro de material relacionado con la explotación sexual de menores que circula en la red. Sin embargo, pese a estos avances, sigue siendo un desafío pendiente evitar que los esfuerzos se dupliquen entre distintos organismos, lo que hace indispensable una mayor coordinación entre redes de cooperación como las del Grupo de los Ocho, Interpol y las instancias vinculadas al Convenio sobre la Ciberdelincuencia.

Hay una realidad que no puede ignorarse: quienes perpetran delitos en entornos digitales se valen de tecnología sofisticada y en constante renovación. Eso obliga a que los investigadores que los persiguen dispongan, cuando menos, de un nivel tecnológico equivalente al de los propios delincuentes y, en la medida

de lo posible, de recursos que los superen. Contar con software y hardware actualizados no es un lujo ni una aspiración secundaria; es una condición mínima para que la lucha contra la ciberdelincuencia tenga alguna posibilidad real de éxito. Por esa razón, dotar a las instituciones investigadoras de estas capacidades debe tratarse como una prioridad que no admite postergación.

2. Fomento de la capacitación: Un aspecto igualmente relevante que fue puesto de relieve es que la amenaza de la criminalidad cibernética trasciende las fronteras de los países con mayor desarrollo económico, alcanzando también a aquellas naciones que aún se encuentran en proceso de consolidación. En esa dirección, los datos recopilados por la Development Gateway Foundation pusieron en evidencia que la cantidad de personas con acceso a internet en los países en desarrollo había llegado a superar a la registrada en las economías más industrializadas del mundo. Esta realidad llevó a que la Asamblea General, por medio de la Resolución 64/179 —instrumento orientado a reforzar el Programa de las Naciones Unidas en materia de prevención del delito y administración de justicia penal—, incorporara dentro de su agenda nuevas categorías de preocupación en el ámbito de la política criminal, tales como la reproducción ilegal de contenidos, la delincuencia en espacios virtuales, la explotación sexual infantil y la inseguridad en contextos urbanos. En ese marco, se exhortó a la Oficina de las Naciones Unidas contra la Droga y el Delito (UNODC) a asumir estas problemáticas como parte de las responsabilidades inherentes a su mandato institucional.

Enfrentar la criminalidad que opera en entornos digitales es una tarea que pone

a prueba las capacidades de todas las instituciones del sistema de justicia. La dificultad no radica únicamente en la naturaleza técnica de los hechos investigados, sino también en que la tecnología evoluciona a un ritmo que muchas veces supera la capacidad de respuesta institucional. Ante eso, mantener una formación continua y actualizada de quienes tienen a su cargo la investigación y el juzgamiento de estos delitos deja de ser una recomendación deseable para convertirse en una exigencia ineludible. En esa línea, el grupo de especialistas de la UNODC ha señalado que consolidar las capacidades de las instituciones involucradas y asegurar que dicha consolidación sea sostenible en el tiempo son factores decisivos al momento de evaluar si las iniciativas emprendidas en este campo están dando resultados reales (Espinoza Calderón, 2022, p. 59).

Pero la formación por sí sola no es suficiente. Las instituciones que tienen la misión de combatir la ciberdelincuencia necesitan también contar con reglas claras que guíen su actuación, lo que implica establecer directrices y protocolos de trabajo, y revisar la legislación procesal y las normas especiales para que estas realmente faciliten la persecución de estos ilícitos en lugar de obstaculizarla. A ello debe sumarse la dotación de los medios logísticos indispensables para que el personal pueda desempeñar su labor en condiciones adecuadas. Solo cuando se conjugan formación, marco normativo actualizado y recursos suficientes es posible hablar de una respuesta institucional verdaderamente eficaz frente a los delitos cibernéticos.

Esta preocupación ha sido recogida también en el plano internacional. El 12.°

Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal colocó en el centro del debate la urgencia de capacitar a los operadores del sistema jurídico -policías, fiscales y jueces- para que puedan afrontar con solvencia la complejidad que caracteriza a este tipo de investigaciones y procesos. Por su parte, en la reunión de expertos de la UNODC sobre ciberdelincuencia llevada a cabo en Viena, se puso de relieve que buena parte de los organismos internacionales y regionales que trabajan en esta área ya han comenzado a tomar medidas concretas para incentivar a quienes se especializan en la investigación de delitos informáticos y para desarrollar materiales formativos que respondan a las necesidades reales del sector.

3. Apoyo de la UNODC: En el marco del 12.° Congreso de las Naciones Unidas sobre Prevención del Delito y Justicia Penal, quedó establecido el papel central que desempeña la UNODC dentro del sistema internacional de lucha contra la criminalidad. Este organismo no actúa como un actor secundario: es la instancia de referencia para la definición de parámetros en materia de prevención del delito y administración de justicia penal, y orienta su asistencia de manera prioritaria hacia aquellos países que aún se encuentran consolidando sus capacidades institucionales en este ámbito. Lo que distingue su enfoque es la voluntad de no fragmentar el problema: la UNODC ha asumido el compromiso de abordar la criminalidad desde una visión que integra simultáneamente los planos jurídico, técnico y operativo, apostando por la colaboración entre distintas disciplinas y actores como condición indispensable para dar respuestas que sean verdaderamente efectivas.

El Perú no estuvo al margen de esta realidad. Consciente de las particularidades que presenta la investigación de los delitos cometidos en entornos digitales, el legislador peruano introdujo a través de la Ley N.° 30096 tres regulaciones específicas orientadas a fortalecer el plano probatorio en estos casos. La primera de ellas extendió a los imputados por delitos informáticos la posibilidad de que el juez disponga la intervención de sus comunicaciones como medida de investigación. La segunda habilitó el uso de la colaboración eficaz en esta clase de ilícitos, dotando así al Ministerio Público de un instrumento adicional para avanzar en sus investigaciones. La tercera reconoció que los mecanismos procesales diseñados para enfrentar la criminalidad organizada también resultan aplicables cuando se trata de delitos informáticos.

Años más tarde, hacia finales del 2020, el Ministerio Público dio un paso institucional relevante al conformar un equipo técnico con la misión de explorar la posibilidad de crear una fiscalía o unidad especializada en este tipo de criminalidad. El trabajo de ese equipo —integrado por fiscales y funcionarios de la institución, con el apoyo técnico de la Embajada de los Estados Unidos— culminó con el nacimiento de la Unidad Fiscal Especializada en Ciberdelincuencia. Desde entonces, esta unidad cumple un rol central en la definición de criterios de actuación, la homogeneización de la interpretación normativa y el respaldo técnico a las investigaciones fiscales vinculadas a delitos informáticos.

Sin embargo, la tarea investigadora del Ministerio Público en este campo tropieza con un obstáculo que no depende de sus propias capacidades: la falta

de colaboración oportuna y completa de entidades del sector bancario, financiero y de telecomunicaciones. Esta situación pone de manifiesto que combatir la ciberdelincuencia no es una responsabilidad que pueda recaer únicamente sobre los operadores del derecho. Se trata de un esfuerzo que exige la participación activa de todos los actores institucionales, facilitando con diligencia la información que requieren el Poder Judicial, el Ministerio Público y la Policía Nacional del Perú para cumplir su función.

Frente a todo lo anterior, resulta evidente que el ordenamiento jurídico tiene una deuda pendiente con la sociedad. La delincuencia tecnológica avanza con una velocidad que el derecho aún no ha logrado igualar, y esa brecha se traduce en impunidad. Los vacíos normativos que persisten en la legislación peruana, y en la de muchos otros países, no son simples deficiencias técnicas: son espacios que los ciberdelincuentes aprovechan y que el Estado no puede seguir tolerando. El elevado número de investigaciones archivadas en etapa preliminar por no haberse logrado identificar al responsable del ilícito es la expresión más concreta de ese fracaso. Por ello, resulta imprescindible que el Estado peruano actúe con decisión y sin demora, diseñando e implementando políticas criminales a la altura de un fenómeno cuyos efectos sobre la sociedad y las instituciones son, a estas alturas, innegables.

2.2 Bases Teóricas

- **La Impunidad de los delitos informáticos**

La impunidad en delitos informáticos se configura como un fenómeno jurídico complejo

que se caracteriza por la ausencia de sanción penal efectiva contra quienes cometen ilícitos utilizando medios tecnológicos o sistemas informáticos. Como señala Villavicencio Terreros (2014), esta problemática surge principalmente por la dificultad en la individualización del ciberdelincuente, lo que genera un estado de desprotección para las víctimas y un mensaje de tolerancia hacia la criminalidad cibernética. La naturaleza transnacional de estos delitos, junto con la sofisticación tecnológica empleada por los criminales, crea desafíos únicos para los sistemas de justicia penal tradicionales.

Que los delitos informáticos queden sin sanción ha dejado de ser una situación anecdótica para convertirse en una preocupación genuina y creciente entre quienes tienen la responsabilidad de legislar, juzgar y acusar. La razón es sencilla pero inquietante: investigar y perseguir este tipo de conductas es extraordinariamente difícil, y esa dificultad, cuando no se enfrenta con los recursos adecuados, termina favoreciendo la impunidad. Detrás de ese resultado no hay una sola causa, sino varias que se alimentan mutuamente. La escasa preparación técnica de quienes operan dentro del sistema judicial, las limitaciones tecnológicas con las que trabajan los investigadores y las deficiencias en los protocolos diseñados para este tipo de delitos configuran un escenario donde los derechos fundamentales de las víctimas quedan expuestos de manera sistemática, sin que el Estado logre ofrecer una respuesta proporcional a la gravedad del daño causado (Huerta Guerrero, 2018).

- **Delitos informáticos en el ordenamiento jurídico peruano**

Los delitos informáticos en el ordenamiento jurídico peruano encuentran su regulación específica en la Ley N° 30096, promulgada en 2013, la cual estableció un marco normativo destinado a prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos. Esta ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos

informáticos, configurándose como la respuesta legislativa del Estado peruano ante el crecimiento exponencial de la criminalidad cibernética. Sin embargo, como advierte Peña Cabrera (2015), la tipificación de estos delitos requiere una interpretación sistemática que considere tanto los elementos tradicionales del tipo penal como las particularidades técnicas de los medios informáticos.

La aplicación práctica de esta normativa presenta serias deficiencias que contribuyen significativamente a la impunidad, particularmente en lo relacionado con la investigación y juzgamiento de estos ilícitos. La complejidad técnica de estos delitos demanda una comprensión especializada que el sistema de justicia peruano aún no ha desarrollado plenamente, generando vacíos de protección que comprometen la efectividad del sistema penal y la protección de los derechos fundamentales de las víctimas (García Toma, 2003).

- **Fraude informático como modalidad delictiva**

El fraude informático constituye una de las modalidades delictivas más comunes dentro del espectro de los delitos cibernéticos, caracterizándose por el uso de medios tecnológicos para obtener un provecho económico ilícito mediante el engaño o la manipulación de sistemas informáticos. Esta conducta delictiva implica la utilización fraudulenta de sistemas informáticos para apropiarse de bienes ajenos, alterando el funcionamiento normal de programas, sistemas o redes informáticas con la finalidad de obtener un beneficio económico indebido. Como señala la doctrina especializada, el fraude informático requiere la concurrencia de elementos típicos específicos que lo diferencian de otras modalidades de estafa tradicional (Peña Cabrera, 2015).

La investigación y persecución del fraude informático presenta desafíos particulares debido a la naturaleza técnica de la evidencia digital y la necesidad de contar con peritos especializados capaces de identificar y preservar las pruebas electrónicas. La impunidad en estos casos se ve

agravada por la dificultad para rastrear las transacciones digitales, la utilización de técnicas de anonimización por parte de los delincuentes, y la falta de coordinación entre las entidades financieras y las autoridades judiciales. Esta problemática compromete directamente el principio constitucional de tutela jurisdiccional efectiva, al dejar sin protección real a las víctimas de estos delitos (Villavicencio Terreros, 2014).

- **Sabotaje informático**

El sabotaje informático constituye una modalidad delictiva específica que se caracteriza por la alteración, interrupción o destrucción maliciosa de sistemas informáticos, redes de comunicación o datos digitales, con la finalidad de causar daño a su funcionamiento normal o comprometer su integridad. Como señala la doctrina especializada en delitos cibernéticos, esta conducta puede manifestarse a través de diversas técnicas como la introducción de virus informáticos, ataques de denegación de servicio, manipulación de software o hardware, y otras formas de interferencia tecnológica que comprometan la operatividad de los sistemas objetivo. El sabotaje informático no solo afecta la integridad técnica de los sistemas, sino que también puede generar consecuencias económicas significativas y comprometer la seguridad de la información (Peña Cabrera, 2015).

La investigación y persecución del sabotaje informático presenta desafíos complejos debido a la sofisticación técnica requerida para identificar los métodos empleados y establecer la autoría de estos actos. La impunidad en estos casos se ve agravada por la necesidad de contar con peritos especializados en sistemas informáticos, la dificultad para preservar la evidencia digital, y la complejidad de los procesos de investigación que requieren conocimientos técnicos avanzados. Esta problemática compromete directamente los principios constitucionales de tutela jurisdiccional efectiva y debido proceso, especialmente cuando las autoridades judiciales carecen de la especialización necesaria para comprender la naturaleza técnica de estos delitos (Villavicencio

Terreros, 2014).

- **Acceso ilícito a sistemas informáticos**

El acceso ilícito a sistemas informáticos, tipificado en el artículo 2° de la Ley N° 30096, se configura como una conducta delictiva que consiste en el acceso sin autorización a todo o parte de un sistema informático, siempre que se realice mediante violación de medidas de seguridad. Según la normativa peruana, la Ley de Delitos Informáticos impone penas de 1 a 4 años de prisión efectiva y 30 a 90 días-multa para el acceso ilícito a sistemas informáticos. La ley peruana define este delito como el acceso no autorizado a sistemas informáticos mediante la vulneración de las medidas de seguridad establecidas, pudiendo realizarse mediante diversas técnicas como el uso de contraseñas obtenidas ilícitamente, la explotación de vulnerabilidades de seguridad, o el empleo de software malicioso diseñado para evadir los controles de acceso.

La persecución penal del acceso ilícito a sistemas informáticos en el ordenamiento jurídico peruano enfrenta obstáculos significativos relacionados con la identificación del origen de los ataques, especialmente cuando se emplean técnicas de anonimización o se utilizan infraestructuras tecnológicas distribuidas geográficamente. Como advierte la doctrina nacional, producto del desarrollo de las tecnologías informáticas se ha ido desarrollando una nueva forma de criminalidad denominada delitos informativos, lo que requiere una respuesta especializada del sistema de justicia peruano. La impunidad en estos casos se ve agravada por las limitaciones técnicas de las autoridades investigadoras para rastrear las conexiones digitales, la falta de especialización del personal fiscal y judicial, y la rapidez con que los perpetradores pueden eliminar las evidencias digitales, comprometiendo gravemente los principios constitucionales de acceso a la justicia y seguridad jurídica (García Toma, 2003).

- **Principios constitucionales fundamentales**

Los principios constitucionales fundamentales constituyen los pilares esenciales que garantizan la correcta administración de justicia y la protección efectiva de los derechos fundamentales de los ciudadanos en un Estado de Derecho. Como expresa García Toma (2003), estos principios operan como mandatos de optimización que orientan la interpretación constitucional y limitan el ejercicio del ius puniendi del Estado, siendo fundamentales para el mantenimiento del orden jurídico constitucional. Entre estos principios se encuentran el derecho al debido proceso, el acceso a la justicia, la tutela jurisdiccional efectiva, la igualdad ante la ley y el principio de legalidad.

La afectación a estos principios constitucionales derivada de la impunidad en delitos informáticos se manifiesta de múltiples formas en el ordenamiento jurídico peruano, generando una crisis de confianza en el sistema de justicia y una vulneración sistemática de los derechos fundamentales. El derecho al debido proceso se ve comprometido cuando las investigaciones no se realizan con la diligencia debida, el acceso a la justicia se vulnera cuando las víctimas no encuentran respuestas efectivas del sistema judicial, y la tutela jurisdiccional efectiva se afecta cuando no existe una protección real y concreta de los derechos vulnerados por los delitos informáticos (Bernales Ballesteros, 2012).

- **Derecho a la intimidad en el entorno digital**

Entre los derechos fundamentales reconocidos por el ordenamiento constitucional peruano, el derecho a la intimidad ocupa un lugar de especial relevancia, encontrando su sustento normativo en el artículo 2°, inciso 7, de la Constitución Política del Perú, disposición que ampara la esfera privada de la persona y su entorno familiar frente a cualquier injerencia que carezca de justificación legítima. En el escenario digital actual, este derecho ha experimentado una notable expansión en su contenido y alcance, extendiéndose hacia la salvaguarda de la información de carácter personal

que se encuentra almacenada en equipos electrónicos, plataformas en línea e infraestructuras informáticas de diversa índole. Al respecto, Landa Arroyo (2014) sostiene que, en el marco de los entornos virtuales, este derecho se traduce en la potestad que asiste a cada individuo de ejercer un dominio efectivo sobre los datos que le pertenecen, determinando de manera autónoma las condiciones bajo las cuales dicha información puede ser conocida, empleada o sometida a algún tipo de tratamiento por parte de terceros.

La vulneración del derecho a la intimidad través de delitos informáticos se manifiesta mediante diversas modalidades como el acceso no autorizado a dispositivos personales, la obtención ilícita de información privada, la interceptación de comunicaciones digitales, y la divulgación no consentida de datos íntimos. La impunidad en estos casos genera una desprotección sistemática de este derecho fundamental, creando un ambiente de inseguridad jurídica donde los ciudadanos carecen de garantías efectivas para la protección de su intimidad en el ámbito digital. Esta situación compromete gravemente el desarrollo de la personalidad y la autonomía individual, elementos esenciales del Estado Constitucional de Derecho (García Belaunde, 2016).

- **Protección de datos personales**

Existe un derecho que, aunque no fue incorporado de manera expresa en el texto original de la Constitución de 1993, ha ganado un reconocimiento progresivo y sólido en el ordenamiento jurídico peruano: el derecho a la protección de los datos personales. Su desarrollo no provino del legislador constituyente, sino de la labor interpretativa del Tribunal Constitucional, que lo fue construyendo a partir de su vinculación con el derecho a la intimidad y con el principio de autodeterminación informativa. Con el tiempo, este derecho encontró también un anclaje normativo específico en la Ley N.° 29733, Ley de Protección de Datos Personales, instrumento que vino a establecer las reglas bajo las cuales debe producirse el tratamiento de la información

personal, exigiendo que este sea lícito, proporcional y transparente. En palabras de Sáenz Dávalos (2017), lo que este derecho garantiza en esencia es la facultad de cada individuo de mantener el control sobre su propia información, pudiendo decidir quién la recoge, cómo se usa y con qué finalidad.

En el contexto de los delitos informáticos, la protección de datos personales se ve gravemente comprometida cuando los sistemas que almacenan información personal son objeto de acceso ilícito, sustracción de datos, o tratamiento no autorizado sin que exista una respuesta penal efectiva. La impunidad en estos casos genera una vulneración sistemática del derecho a la autodeterminación informativa, al permitir que terceros no autorizados accedan, utilicen y dispongan de información personal sin el consentimiento de los titulares y sin consecuencias penales efectivas. Esta situación compromete elementos esenciales como la confidencialidad, integridad y disponibilidad de los datos personales (Remotti Carbonell, 2018).

- **Secreto de las comunicaciones**

El secreto de las comunicaciones, consagrado en el artículo 2° inciso 10 de la Constitución Política del Perú, constituye un derecho fundamental que garantiza la inviolabilidad de las comunicaciones privadas, abarcando tanto las comunicaciones tradicionales como las efectuadas a través de medios digitales y electrónicos. Este derecho implica la prohibición de interceptación, grabación, divulgación o utilización de comunicaciones privadas sin autorización judicial previa y por motivos expresamente establecidos en la ley. Como señala Quiroga León (2014), el secreto de las comunicaciones es esencial para el libre desarrollo de la personalidad y la intimidad de las personas, constituyendo un límite infranqueable para la actuación del Estado y de los particulares.

En el ámbito de los delitos informáticos, el secreto de las comunicaciones se ve vulnerado mediante diversas modalidades como la interceptación ilegal de comunicaciones electrónicas, el

acceso no autorizado a cuentas de correo electrónico, la intervención de comunicaciones en redes sociales y aplicaciones de mensajería, y la obtención ilícita de registros de comunicaciones digitales. La impunidad en estos casos genera una desprotección sistemática de este derecho fundamental, comprometiendo la confidencialidad de las comunicaciones privadas y creando un ambiente de desconfianza en los medios de comunicación digital (Bernales Ballesteros, 2012).

- **Debido proceso como garantía constitucional**

Toda persona que se ve involucrada en un proceso judicial o administrativo, ya sea como imputada, como víctima o como parte, tiene derecho a que ese proceso se desarrolle con ciertas garantías mínimas que el Estado no puede ignorar ni recortar. Eso es, en esencia, lo que protege el debido proceso: la certeza de que quien comparece ante la justicia será escuchada, podrá ejercer su defensa en condiciones adecuadas y recibirá una resolución de parte de un tribunal que sea competente, independiente de presiones externas e imparcial frente a las partes. El artículo 139°, inciso 3, de la Constitución Política del Perú recoge este principio y lo convierte en una exigencia vinculante para el Estado, estableciendo un estándar por debajo del cual ningún proceso, sea cual sea su naturaleza, puede descender sin violar la Constitución. Como señala García Belaunde (2016), estas reglas no son formalidades vacías: son el escudo que tienen las personas frente a cualquier actuación del poder público que pudiera afectar sus derechos, y su observancia es lo que distingue a un sistema de justicia legítimo de uno que opera de manera arbitraria.

En el contexto de los delitos informáticos, el debido proceso adquiere una dimensión especial debido a la complejidad técnica de estos ilícitos y la necesidad de garantizar que las investigaciones se realicen con la diligencia debida y el rigor científico requerido. La vulneración de este principio se materializa cuando los operadores de justicia carecen de la especialización necesaria para comprender la naturaleza técnica de estos delitos, cuando se archivan

prematuramente las investigaciones por falta de capacidades técnicas, o cuando no se emplean los medios probatorios adecuados para el esclarecimiento de los hechos (Landa Arroyo, 2014).

- **Principio de legalidad penal**

Pocas máximas han tenido una influencia tan duradera en el derecho penal como la expresada en el aforismo latino *nullum crimen, nulla poena sine lege*. Su vigencia no ha disminuido con el paso del tiempo; por el contrario, sigue siendo uno de los fundamentos sobre los que descansa cualquier sistema punitivo que aspire a ser legítimo dentro de un Estado de Derecho. Lo que este principio establece es, en esencia, una prohibición dirigida al propio Estado: ninguna conducta puede ser tratada como delito si no ha sido previamente definida como tal por la ley, y ninguna persona puede ser sometida a una pena que no estuviera ya prevista antes de que ocurrieran los hechos que se le imputan. Villavicencio Terreros (2014) destaca que esta garantía cumple una función protectora de primer orden, pues al fijar límites precisos al ejercicio del poder punitivo estatal, otorga a los ciudadanos la certeza de saber qué conductas están prohibidas y qué consecuencias acarrea su transgresión.

Cuando este principio se traslada al terreno de los delitos informáticos, su aplicación se vuelve especialmente exigente. La tecnología no se detiene, y con ella surgen permanentemente nuevas formas de delinquir que el legislador no siempre logra anticipar. Eso coloca al derecho penal ante una tensión difícil de resolver: los tipos penales deben ser lo suficientemente amplios para no dejar sin respuesta conductas dañosas, pero al mismo tiempo deben ser claros y precisos para no caer en la arbitrariedad que el principio de taxatividad precisamente busca evitar. Cuando esa técnica legislativa falla —cuando las normas son vagas, desactualizadas o incompletas, el resultado casi inevitable es la impunidad, no porque el sistema no quiera sancionar, sino porque carece de los instrumentos legales adecuados para hacerlo (Peña Cabrera, 2015).

- **Seguridad Jurídica**

La seguridad jurídica constituye un principio fundamental del Estado de Derecho que garantiza la certidumbre, predictibilidad y estabilidad del ordenamiento jurídico, permitiendo a los ciudadanos conocer con anticipación las consecuencias jurídicas de sus actos y tener confianza en la efectividad del sistema legal. Como expresa Landa Arroyo (2014), la seguridad jurídica implica que las normas jurídicas sean claras, públicas, estables y aplicadas de manera consistente por los órganos del Estado, generando un ambiente de confianza institucional que favorece el desarrollo social y económico. Este principio se encuentra íntimamente relacionado con otros principios constitucionales como la legalidad, la igualdad ante la ley y la tutela jurisdiccional efectiva.

En el contexto de los delitos informáticos, la seguridad jurídica se ve gravemente comprometida por los altos índices de impunidad que caracterizan este tipo de ilícitos, generando una percepción de que el ordenamiento jurídico es ineficaz para proteger a los ciudadanos en el entorno digital. La falta de respuestas efectivas del sistema de justicia ante los delitos cibernéticos erosiona la confianza ciudadana en las instituciones y crea incentivos perversos para la proliferación de estas conductas delictivas, afectando así el deber del Estado de garantizar la seguridad de las personas y la efectividad del sistema legal (García Belaunde, 2016).

- **Estado Constitucional de Derecho**

El Estado Constitucional de Derecho representa la evolución más avanzada del concepto clásico de Estado de Derecho, caracterizándose por el reconocimiento de la supremacía constitucional y la sujeción de todos los poderes públicos a los principios y valores constitucionales. El Estado Constitucional de Derecho tiene sobre todo a la persona humana y el respeto de su dignidad como el fin supremo de la sociedad y del Estado, con libertades y derechos reconocidos y con la existencia de mecanismos de garantía eficaces para su protección. En este

modelo, la Constitución no solo establece la organización del poder político, sino que también consagra un catálogo de derechos fundamentales y establece mecanismos eficaces para su protección y garantía.

En el contexto peruano, la consolidación del Estado Constitucional de Derecho implica que todas las actuaciones del Estado, incluyendo la persecución penal de los delitos informáticos, deben estar orientadas por los principios constitucionales y dirigidas a la protección efectiva de los derechos fundamentales. La impunidad en delitos cibernéticos constituye una manifestación de las deficiencias del Estado para cumplir con su deber constitucional de garantizar la seguridad y protección de los ciudadanos, comprometiendo así la legitimidad y eficacia del modelo constitucional adoptado por el ordenamiento jurídico peruano (García Toma, 2003).

- **Derecho administrativo y constitucionalización**

El derecho administrativo en su configuración actual atraviesa un proceso de profunda transformación, caracterizado por la progresiva incorporación de los principios y valores de rango constitucional como parámetros vinculantes de toda la actividad que despliega el aparato estatal. Esta evolución ha supuesto una ruptura con la visión clásica de la administración pública, redefiniéndola a partir de una lógica de sujeción integral al texto constitucional. En ese marco, el principio de legalidad se erige como el eje vertebrador del derecho administrativo, al imponer a todas las autoridades que conforman el Estado —sin distinción de su naturaleza o jerarquía— el deber de orientar su actuación con plena observancia de la Constitución, el ordenamiento legal vigente y el derecho en su conjunto. Esta exigencia no se agota en la mera conformidad formal con la norma escrita, sino que se extiende al respeto activo y la promoción efectiva de los derechos fundamentales en cada una de las decisiones y actuaciones que emanan del poder público.

En lo que atañe específicamente a la persecución de la criminalidad informática, esta

constitucionalización del derecho administrativo se expresa en la obligación que recae sobre las autoridades competentes, entre ellas fiscales y magistrados, de conducir su labor con irrestricta sujeción a garantías como el debido proceso, la tutela jurisdiccional efectiva y el acceso igualitario a la justicia. Cuando la impunidad se instala como una constante en el tratamiento de estos delitos, ello revela una disfunción estructural del sistema de justicia que compromete el cumplimiento de los mandatos constitucionales más esenciales, poniendo de manifiesto la urgencia de acometer reformas de fondo que aseguren la vigencia real de dichos principios frente al avance de la ciberdelincuencia (Landa Arroyo, 2014).

- **Habeas data como garantía constitucional**

Dentro del catálogo de garantías constitucionales que reconoce el ordenamiento jurídico peruano, el habeas data ocupa un lugar singular al encontrarse expresamente regulado en el artículo 200°, inciso 3, de la Constitución Política del Perú. Su finalidad esencial consiste en brindar amparo a los derechos vinculados tanto al acceso a la información de carácter público como a la tutela de los datos de naturaleza personal. A través de esta figura, cualquier persona se encuentra facultada para requerir el acceso a información que le concierne y que obra en registros o bases de datos administradas por entidades de naturaleza pública o privada, pudiendo igualmente exigir la eliminación, corrección, reserva o actualización de aquellos datos que resulten inexactos o que vulneren ilegítimamente sus derechos. En palabras de Landa Arroyo (2012), esta garantía se configura como el instrumento procesal idóneo para la defensa de los derechos informáticos y el ejercicio de la autodeterminación informativa por parte de los ciudadanos.

En el escenario de la criminalidad informática, el habeas data cobra una dimensión particularmente relevante al operar como un mecanismo de protección que actúa en forma complementaria al proceso penal, otorgando a quienes han sido víctimas de delitos cibernéticos la

posibilidad de conocer el tratamiento al que han sido sometidos sus datos personales y de reclamar las medidas correctivas que correspondan ante cualquier vulneración detectada. No obstante, la eficacia práctica de esta garantía se ve severamente limitada por la persistencia de la impunidad en materia de delitos informáticos, dado que la inexistencia de consecuencias penales concretas disminuye considerablemente los incentivos para acatar de manera voluntaria las decisiones emitidas en el marco de los procesos de habeas data, debilitando con ello la protección integral de los derechos informáticos de los ciudadanos (García Belaunde, 2016).

- **Proporcionalidad en la investigación de delitos informáticos**

Cuando en el marco de una investigación penal entran en colisión distintos derechos fundamentales, el sistema jurídico necesita de un criterio que permita resolver esa tensión sin sacrificar ninguno de ellos de manera innecesaria. Ese papel lo cumple el principio de proporcionalidad, cuya relevancia se torna especialmente evidente en el ámbito de los delitos informáticos, donde la eficacia de la persecución penal puede chocar frontalmente con derechos tan sensibles como la intimidad o la protección de los datos personales. El Tribunal Constitucional ha ido perfilando este principio a través de su jurisprudencia, estableciendo que toda medida que implique una restricción de derechos fundamentales debe superar un triple examen: ha de ser idónea para alcanzar el objetivo que la justifica, ha de ser la menos gravosa entre las alternativas disponibles, y ha de guardar una proporción razonable entre el beneficio que persigue y el costo que impone. Sáez Dávalos (2017) subraya que, en definitiva, este principio opera como un límite frente a cualquier actuación estatal que pretenda restringir derechos de manera excesiva o sin justificación suficiente.

Esta exigencia cobra una dimensión especialmente crítica cuando lo que se investiga son precisamente conductas que han afectado la intimidad, el secreto de las comunicaciones o la

información personal de las víctimas. En esos casos, las diligencias de investigación deben ser diseñadas y ejecutadas con particular cuidado, de modo que el propio proceso de esclarecimiento de los hechos no termine convirtiéndose en una nueva fuente de vulneración para quienes ya resultaron afectados. Porque cuando las medidas investigativas se aplican sin respetar el principio de proporcionalidad, puede ocurrir algo paradójico: que el daño causado por la investigación supere al causado por el delito mismo, poniendo en entredicho la legitimidad constitucional de todo el proceso penal (Villavicencio Terreros, 2014).

2.3. Bases filosóficas

Comprender por qué la impunidad en delitos informáticos representa algo más que una simple falla del sistema penal exige ir más allá del análisis normativo y preguntarse por los fundamentos filosóficos que sostienen el derecho constitucional y administrativo en su configuración actual. Dos corrientes resultan especialmente iluminadoras para este propósito: el constitucionalismo moderno y la teoría de los derechos fundamentales. Ambas comparten una preocupación central: establecer límites al poder del Estado y asegurar que esos límites no sean meramente declarativos, sino que se traduzcan en una protección real y efectiva de los derechos de las personas. Desde esa perspectiva, la impunidad en el ámbito digital no es un problema técnico o presupuestario: es una cuestión que toca la legitimidad misma del ordenamiento jurídico, pues cuando el Estado es incapaz de garantizar principios como la tutela jurisdiccional efectiva, la seguridad jurídica o la igualdad ante la ley, el contrato social sobre el que descansa su autoridad comienza a resquebrajarse.

El constitucionalismo moderno, cuyas bases fueron sentadas por pensadores como Ronald Dworkin y Robert Alexy, propone una visión del texto constitucional que va mucho más allá de su dimensión normativa formal. La Constitución, desde esta perspectiva, no es

simplemente la norma de mayor jerarquía dentro del ordenamiento; es un sistema de principios y valores que impregna y orienta la totalidad del derecho, irradiando sus exigencias hacia cada rama del ordenamiento jurídico y hacia cada actuación de los poderes públicos. Los principios constitucionales, en este esquema, no son simples recomendaciones: tienen fuerza normativa directa y obligan tanto a las instituciones del Estado como a los particulares. Alexy (2007) los caracteriza como mandatos de optimización, es decir, directrices que deben realizarse en la mayor medida que las circunstancias permitan. Aplicado al problema de los delitos informáticos, este planteamiento tiene una consecuencia clara: el Estado no puede escudarse en sus limitaciones tecnológicas o en restricciones presupuestarias para justificar su inacción. Tiene la obligación constitucional de desarrollar los mecanismos necesarios para que los derechos fundamentales de los ciudadanos sean efectivamente protegidos también en el entorno digital.

La teoría de los derechos fundamentales, particularmente en su dimensión objetiva desarrollada por la doctrina alemana y adoptada por diversos sistemas constitucionales, establece que estos derechos no solo constituyen esferas subjetivas de protección individual, sino también mandatos objetivos que obligan al Estado a crear las condiciones institucionales y normativas necesarias para su efectiva realización. Esta dimensión objetiva implica deberes positivos de protección que exigen al Estado adoptar medidas legislativas, administrativas y judiciales adecuadas para prevenir y sancionar las vulneraciones de derechos, incluso cuando provengan de terceros privados. En el ámbito de los delitos informáticos, esta teoría fundamenta la obligación estatal de desarrollar marcos normativos especializados y capacidades institucionales apropiadas para enfrentar las nuevas formas de criminalidad digital. (Häberle, 2003)

El neoconstitucionalismo, como corriente que enfatiza la centralidad de los principios constitucionales y la interpretación evolutiva de la Constitución, proporciona el marco filosófico desde el cual se aborda esta investigación. Esta perspectiva sostiene que la Constitución debe adaptarse a los nuevos desafíos sociales y tecnológicos sin perder su fuerza normativa, lo que implica que los principios constitucionales tradicionales deben ser reinterpretados para ofrecer respuestas efectivas a problemáticas contemporáneas como la criminalidad informática. La investigación se fundamenta en esta corriente al analizar cómo la impunidad digital constituye una vulneración del mandato constitucional de protección efectiva de derechos y al proponer mecanismos de fortalecimiento institucional que permitan actualizar la respuesta estatal sin alterar la estructura constitucional vigente, garantizando así la coherencia del sistema jurídico y la vigencia plena del Estado constitucional de derecho.

2.4. Definición de términos básicos

- **La Impunidad**

Cuando una persona comete un delito y no recibe ninguna consecuencia por ello, no estamos únicamente ante una falla del sistema penal: estamos ante un problema que toca los cimientos mismos del Estado de derecho. La impunidad, entendida como la ausencia de respuesta punitiva frente a conductas que el ordenamiento jurídico prohíbe, no es un fenómeno neutral. Su persistencia deteriora la vigencia efectiva de las normas y envía un mensaje silencioso pero devastador a la sociedad: que las leyes no siempre se cumplen y que el Estado no siempre cumple su promesa de hacer justicia.

Desde una perspectiva constitucional, el problema va más allá de la simple falta de sanción. Cuando la impunidad se instala, no solo queda sin castigo el responsable del delito; también quedan sin protección real principios que la Constitución reconoce como esenciales, entre ellos la tutela

jurisdiccional efectiva y la igualdad de todas las personas ante la ley. Sus manifestaciones son variadas: puede presentarse como una deficiencia normativa, cuando el ordenamiento carece de tipos penales suficientemente precisos para abarcar ciertas conductas; como una falla institucional, cuando los organismos encargados de la persecución penal no cuentan con los medios o la capacidad para cumplir su función; o como un obstáculo procesal, cuando la tramitación de los casos se ve bloqueada por trabas que impiden llegar a una resolución oportuna.

Lo más preocupante, sin embargo, es cuando estas fallas dejan de ser excepcionales y se vuelven sistemáticas. En ese punto, la impunidad ya no es solo un problema jurídico: se convierte en un fenómeno social que erosiona la confianza de los ciudadanos en sus instituciones y cuestiona la legitimidad del propio Estado constitucional de derecho.

- **Delitos informáticos**

Los delitos informáticos constituyen un conjunto de conductas antijurídicas que se caracterizan por el uso de sistemas informáticos, redes de comunicación o tecnologías digitales como medio, objeto o finalidad de la acción delictiva. Estos ilícitos penales abarcan desde accesos no autorizados a sistemas informáticos, manipulación de datos, fraude electrónico, hasta la difusión de contenido ilegal a través de medios digitales. La particularidad de estos delitos radica en su naturaleza transnacional, su capacidad de causar daños masivos en períodos muy breves, y la complejidad técnica que requieren para su investigación y persecución. Desde una perspectiva constitucional, los delitos informáticos plantean desafíos específicos para la protección de derechos fundamentales como la intimidad, el honor, la protección de datos personales y la seguridad jurídica, requiriendo que el Estado desarrolle capacidades institucionales especializadas para garantizar una respuesta eficaz que no comprometa las garantías constitucionales del debido proceso.

- **Principios constitucionales**

Dentro del ordenamiento jurídico, no todas las normas funcionan de la misma manera. Las reglas operan de forma binaria: se cumplen o no se cumplen. Los principios, en cambio, tienen una lógica distinta y más compleja. Son expresión de los valores más profundos que una sociedad ha decidido consagrar en su Constitución, y su fuerza no depende de que estén formulados con precisión quirúrgica, sino de que irradian su contenido hacia todo el sistema legal, condicionando la interpretación y la aplicación de cualquier norma que forme parte de él. Tanto los poderes públicos como los particulares quedan vinculados por ellos, sin excepción. Alexy los describió con precisión al caracterizarlos como mandatos de optimización: no exigen un cumplimiento absoluto e incondicional, sino la realización de su contenido en la mayor medida que las circunstancias, tanto fácticas como jurídicas, permitan.

En el ámbito de la administración de justicia, principios como la tutela jurisdiccional efectiva, el debido proceso, la igualdad ante la ley, la proporcionalidad y la seguridad jurídica no se limitan a funcionar como barreras frente al abuso del poder estatal. También generan obligaciones positivas: el Estado no solo debe abstenerse de vulnerarlos, sino que debe actuar activamente para garantizar su vigencia real. Cuando eso no ocurre, cuando estos principios son sistemáticamente comprometidos por la incapacidad del sistema de justicia para responder con eficacia, las consecuencias van más allá del daño individual que sufre cada víctima concreta. Lo que se resiente es la dimensión objetiva del propio ordenamiento constitucional: la Constitución pierde eficacia normativa, y el Estado constitucional de derecho, que en teoría la garantiza, comienza a debilitarse desde adentro.

- **Tutela jurisdiccional efectiva**

La tutela jurisdiccional efectiva es un principio constitucional fundamental que garantiza el

derecho de toda persona a acceder a la justicia y obtener una respuesta fundada en derecho por parte de los órganos jurisdiccionales competentes. Este principio comprende tanto una dimensión formal (acceso a los tribunales) como una dimensión material (obtención de una decisión de fondo motivada y ejecutable). La tutela jurisdiccional efectiva implica que el Estado debe proporcionar mecanismos procesales adecuados, órganos jurisdiccionales competentes y procedimientos que permitan la protección real de los derechos e intereses legítimos de los justiciables. En el ámbito de los delitos informáticos, este principio exige que el sistema de justicia cuente con las herramientas normativas, técnicas y humanas necesarias para investigar, procesar y sancionar eficazmente estas conductas delictivas, pues la imposibilidad de obtener justicia en casos de criminalidad digital constituye una vulneración directa de este derecho fundamental y genera una situación de desprotección incompatible con el Estado constitucional de derecho.

- **Debido proceso**

El debido proceso constituye un principio constitucional fundamental que garantiza que toda persona sometida a un procedimiento judicial o administrativo tenga derecho a ser tratada con las formalidades y garantías que establece la ley, asegurando así la regularidad y legitimidad de la actividad estatal. Este principio comprende tanto una dimensión formal (observancia de los procedimientos establecidos) como una dimensión sustantiva (razonabilidad y proporcionalidad de las decisiones). El debido proceso incluye garantías como el derecho de defensa, la presunción de inocencia, el derecho a ser oído, la motivación de las resoluciones, la pluralidad de instancia y el derecho a la prueba. En el contexto de la persecución de delitos informáticos, el debido proceso exige que las autoridades respeten escrupulosamente estos derechos, incluso cuando utilicen técnicas especializadas de investigación digital, garantizando que la búsqueda de eficacia en la lucha contra la criminalidad informática no comprometa las garantías fundamentales que protegen

a los ciudadanos frente al ejercicio del poder punitivo estatal.

- **Seguridad jurídica**

Uno de los elementos que distingue a un Estado verdaderamente sometido al derecho es la capacidad de ofrecer a sus ciudadanos algo que va más allá de las normas escritas: la certeza de que esas normas son reales, estables y predecibles. A eso apunta la seguridad jurídica como principio constitucional. Su contenido no se agota en la existencia formal de leyes; exige que estas sean comprensibles, accesibles y suficientemente precisas para que cualquier persona pueda conocer de antemano qué está permitido, qué está prohibido y qué consecuencias acarrea actuar de una u otra manera. Pero, además, exige que quienes aplican el derecho lo hagan de forma coherente y uniforme, sin que los resultados varíen caprichosamente según el caso o el funcionario de turno. En esa misma línea, la seguridad jurídica también protege la confianza que los ciudadanos depositan en la actuación de los poderes públicos y la estabilidad de las situaciones que el propio ordenamiento ha consolidado.

Cuando este principio se traslada al terreno de los delitos informáticos, sus exigencias se vuelven especialmente concretas. Las normas que tipifican estas conductas deben estar formuladas con suficiente claridad para que no haya lugar a dudas sobre qué comportamientos están sancionados. Los procedimientos de investigación y juzgamiento deben ser predecibles y respetar en todo momento las garantías constitucionales de quienes intervienen en ellos. Y el Estado debe ser capaz de hacer cumplir esas normas de manera efectiva. Cuando esto no ocurre, cuando la impunidad se convierte en la respuesta habitual frente a la criminalidad digital, la seguridad jurídica queda gravemente comprometida. No porque las leyes hayan desaparecido del papel, sino porque han perdido su capacidad de operar en la realidad, generando una incertidumbre que ningún ordenamiento constitucional serio puede permitirse ignorar.

2.5. Hipótesis de investigación

2.5.1. Hipótesis general

La impunidad de los delitos informáticos se relacionaría significativamente con su afectación a los Principios constitucionales del Distrito Fiscal de Lima Centro, 2024.

2.5.2. Hipótesis específicas

He1: El fraude informático se relacionaría significativamente con su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024.

He2: El sabotaje informático se relacionaría significativamente con su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024.

He3: El acceso ilícito se relacionaría significativamente con su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024.

2.5.3. Variables de investigación

Variable Independiente (Vi): Delitos Informáticos

Variable Dependiente (Vd): Principios constitucionales

2.6. Operacionalización de variables

<table>
<tr><th rowspan="2">Hipótesis</th><th rowspan="2">Variables</th><th colspan="2">Definición</th><th>Dimensiones</th><th>Indicadores</th><th rowspan="2">Técnica de recolección de datos</th></tr>
<tr><th>Conceptual</th><th>Operacional</th><th></th><th></th></tr>
<tr><td rowspan="11">La impunidad de los delitos informáticos se relacionaría significativamente con su afectación a los Principios constitucionales del Distrito Fiscal de Lima Centro, 2024.</td><td rowspan="6">Variable Independiente:
Delitos Informáticos</td><td rowspan="6">Conductas delictivas que utilizan las tecnologías de la información y comunicación como medio, objeto o finalidad para vulnerar bienes jurídicos protegidos, incluyendo el acceso ilícito a sistemas, manipulación de datos y fraude electrónico.</td><td rowspan="6">Esta variable será medida con la técnica de la encuesta y el análisis documental.</td><td rowspan="2">Fraude informático</td><td>Phishing</td><td rowspan="11">Técnica:
- Ficha de análisis.
- Encuesta.
Instrumento:
- Análisis documental.
- Cuestionario de preguntas.</td></tr>
<tr><td>Fraude de tarjetas</td></tr>
<tr><td rowspan="2">Sabotaje informático</td><td>Espionaje informático</td></tr>
<tr><td>Programas informáticos</td></tr>
<tr><td rowspan="2">Acceso ilícito</td><td>Interceptación</td></tr>
<tr><td>Hacking</td></tr>
<tr><td rowspan="5">Variable Dependiente:
Principios constitucionales</td><td rowspan="5">Postulados fundamentales establecidos en la Constitución que limitan el ejercicio del poder punitivo del Estado, garantizando el respeto a los derechos fundamentales en la persecución y sanción de delitos, tales como legalidad, debido proceso y proporcionalidad de las penas.</td><td rowspan="5">Esta variable será medida con la técnica de la encuesta.</td><td rowspan="2">Derecho a la intimidad</td><td>Privacidad</td></tr>
<tr><td>Reserva</td></tr>
<tr><td rowspan="2">El secreto a las comunicaciones</td><td>Dignidad</td></tr>
<tr><td>Reputación</td></tr>
<tr><td rowspan="2">Protección de datos personales</td><td>Confidencialidad</td></tr>
<tr><td>Derecho al Honor</td></tr>
</table>

Nota. Elaboración propia

Capítulo III: Metodología

3.1. Diseño metodológico

3.1.1. Tipo de la investigación

Básica: La presente investigación es de tipo básica debido a que busca generar conocimiento y ampliar el marco teórico existente sobre la impunidad de los delitos informáticos y su relación con los principios constitucionales. Según Carrasco (2005), la investigación básica "está orientada a lograr un nuevo conocimiento de manera sistemática, con el único propósito de acrecentar el caudal de conocimientos de una determinada disciplina" (p. 43). En este sentido, la investigación contribuirá al conocimiento jurídico constitucional y administrativo.

3.1.2. Nivel de investigación

Descriptivo-correlacional: Desde el plano descriptivo, este nivel de investigación posibilita la caracterización detallada de la situación de impunidad en materia de criminalidad informática, así como de sus repercusiones sobre los principios de jerarquía constitucional en el ámbito del Distrito Fiscal de Lima Centro. El componente correlacional, por su parte, tiene como propósito establecer el grado de vinculación existente entre ambas variables objeto de estudio. En ese sentido, Hernández, Fernández y Baptista (2014) precisan que los estudios de esta naturaleza establecen asociaciones entre variables a partir de patrones que pueden identificarse en un grupo o colectivo determinado (p. 93), lo que permite valorar el nivel de correspondencia entre dos o más categorías, conceptos o variables dentro de una misma investigación.

3.1.3. Diseño de la investigación

No experimental: A lo largo del proceso investigativo no se realizó intervención alguna sobre la unidad de análisis, manteniéndose una postura estrictamente observacional. Hernández (2014) sostiene que esta modalidad investigativa comprende aquellos estudios en los que las variables permanecen intactas, sin ser objeto de ningún tipo de manipulación deliberada, procediendo únicamente a la observación de los hechos en su entorno habitual con miras a su posterior examen.

3.1.4. Enfoque de la investigación

Mixto: La presente investigación adopta una perspectiva metodológica mixta, que articula elementos de naturaleza cualitativa y cuantitativa con el fin de lograr una comprensión global del fenómeno objeto de estudio. El componente cuantitativo posibilitará la medición y el examen estadístico de la relación existente entre las variables, en tanto que el componente cualitativo aportará profundidad al análisis de los aspectos jurídicos y constitucionales que se encuentran involucrados. En palabras de Creswell (2003), esta modalidad metodológica supone la recopilación, el procesamiento y la integración de datos tanto cuantitativos como cualitativos en el marco de un mismo estudio (p. 15).

3.2. Población y muestra

3.2.1. Población de estudio

La población considerada para este estudio estuvo conformada por los operadores jurídicos del Distrito Fiscal de Lima Centro que mantienen vinculación directa con la investigación y el procesamiento de delitos informáticos, ascendiendo a un total de 180 profesionales.

3.2.2. Muestra

Según lo planteado por Valdivia (2018), la muestra puede concebirse como un subconjunto representativo que se extrae de una población o universo determinado, el cual condensa las propiedades esenciales del total, haciendo posible que los hallazgos obtenidos puedan ser proyectados al conjunto más amplio del que proviene (p. 334). Una vez establecidos los límites de la población correspondiente a la unidad de análisis, el procedimiento de selección de las unidades muestrales se efectuó aplicando la técnica propia de la muestra de unidad de análisis.

Con el fin de precisar la cantidad de operadores jurídicos del Distrito Fiscal de Lima Centro a quienes se administró el cuestionario como herramienta de recolección de datos, se hizo uso de la siguiente expresión estadística:

$$n = \frac{\text{p x q x } Z^2\text{x N}}{Z^2 \; x \; p \; x \; q + e^2 \; (N-1)}$$

Leyenda:

n= Tamaño total de la muestra

N= Tamaño total de la población considerada

p y q= Desviación estándar poblacional; ante la ausencia de un valor conocido, se emplea el valor constante de 0.5 (Valor estándar = 0.5)

Z= Constante asociada al nivel de confianza seleccionado; cuando no se dispone de datos estadísticos, se utiliza el valor de 1.96, equivalente a un nivel de confianza del 95%, o 2.58 para un nivel del 99%, según criterio del investigador.

e = Margen de error muestral aceptable, habitualmente comprendido entre el 1%

(0.01) y el 10% (0.10), seleccionable por el investigador en ausencia de un valor estadístico específico.

Muestra de la Unidad de Análisis**:**

$$n_0 = \frac{0.5.x\ 0.5\ x\ (1.96)^2\ x\ 180}{(1.96)^2\ x\ 0.5\ x\ 0.5+(0.1)^2\ (180-1)}$$

$$n_0 = \frac{0.9604\ x\ 180}{0.9604 + 0.01\ x\ 179}$$

$$n_0 = \frac{172.872}{2.7504}$$

$$n_0 = 62.85$$

$$n_0 = 63$$

n_0 = El tamaño resultante de la muestra es de **63 operadores jurídicos** del Distrito Fiscal de Lima Centro.

3.3. Técnicas de recolección de datos

3.3.1. Técnicas a emplear

El presente estudio hizo uso de la encuesta como técnica central de recolección de información.

Encuesta: De acuerdo con Arias (2016), esta técnica se inscribe de manera característica dentro del diseño de investigación de campo (p. 34). Su elección para el presente trabajo respondió a su idoneidad frente a los objetivos planteados, pues tal como lo explica Olvera (2015), se trata de un procedimiento metódico mediante el cual el investigador dirige una serie de preguntas a los participantes del estudio con la finalidad de obtener los datos necesarios, los cuales son posteriormente agrupados y sometidos a un proceso de valoración

(p. 121).

3.3.2. Descripción de los instrumentos

Cuestionario de preguntas: Como instrumento de recolección se utilizó un cuestionario estructurado en base a preguntas de tipo cerrado, cuyas opciones de respuesta se organizaron siguiendo los criterios de la escala de Likert. Sobre este tipo de herramienta, Olvera (2015) indica que su principal ventaja radica en la posibilidad de concentrar y sistematizar las respuestas obtenidas para expresarlas posteriormente en términos numéricos, facilitando así su tratamiento estadístico (p. 125).

- **Escala valorativa**

Escala de Likert: Esta herramienta de medición se construye a partir de una serie de enunciados frente a los cuales cada participante debe pronunciarse eligiendo una entre cinco alternativas dispuestas jerárquicamente (Barrantes, 2018). Para los fines de la presente investigación, dichas opciones fueron ordenadas de manera progresiva, partiendo del menor al mayor grado de conformidad con las afirmaciones planteadas, conforme se detalla en el cuadro siguiente:

Totalmente en desacuerdo	En desacuerdo	Ni de acuerdo ni en desacuerdo	De acuerdo	Totalmente de acuerdo
1	2	3	4	5

3.3.3. Validez y confiabilidad del instrumento de recolección de datos

- **Alfa de Cronbach:** A efectos de establecer el nivel de confiabilidad del instrumento empleado, se recurrió al coeficiente alfa de Cronbach, estadístico que se muestra especialmente adecuado en situaciones donde las opciones de respuesta son de naturaleza

policotómica, como ocurre con los ítems estructurados bajo la escala Likert. Los valores que puede adoptar este coeficiente oscilan en un rango que va de 0 a 1, donde el extremo inferior refleja una confiabilidad nula y el extremo superior denota una confiabilidad plena del instrumento.

$$\alpha = \frac{K}{K-1}\left[1-\frac{\sum S_i^{\,2}}{S_T^{\,2}}\right]$$

Ahora bien, la interpretación de la magnitud del Coeficiente de Confiabilidad de un instrumento responde a los siguientes parámetros:

Tabla 1. Magnitud del Coeficiente Alfa de Cronbach

Rangos	Magnitud
0.81 a 1.00	**Muy alta**
0.61 a 0.80	Alta
0.41 a 0.60	Moderada
0.21 a 0.40	Baja
0.01 a 0.20	Muy baja

Nota. Parámetros para determinar confiabilidad del instrumento

Tabla 2. Resumen de procesamiento de casos

Resumen de procesamiento de casos			
		N	%
Casos	Válido	63	100,0
	Excluido[a]	0	,0
	Total	63	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Nota. Alfa de Cronbach

Tabla 3. Estadística de fiabilidad

Estadísticas de fiabilidad	
Alfa de Cronbach	N de elementos
,842	12

Nota. El valor obtenido del Alfa de Cronbach fue de **0.842**, lo que refleja una magnitud **Muy Alta** de confiabilidad, ubicándose dentro del rango superior de la escala de medición establecida.

3.4. Técnicas para el procesamiento y análisis de la información

3.4.1. Plan de procesamiento de datos

Durante el desarrollo de la investigación se acumuló un conjunto de datos que no podían ser utilizados en bruto, sino que necesitaron pasar por un proceso cuidadoso de análisis, ordenamiento y evaluación. Solo a través de ese tratamiento fue posible extraer conclusiones significativas, detectar tendencias y encontrar respuestas al problema que motivó el estudio. Este trabajo con los datos es también el que permitió al investigador construir propuestas de solución que no sean meramente teóricas, sino que tengan viabilidad y aplicabilidad en la realidad concreta. Para llevar a cabo este proceso de manera ordenada, se distinguieron tres momentos sucesivos:

En primer lugar, la **fase de entrada**, que correspondió al momento en que la información recopilada fue organizada y dispuesta de manera sistemática, sentando las bases para el trabajo estadístico y optimizando la carga al momento de procesar los datos.

En segundo lugar, la **fase de proceso**, en la que se trabajó sobre el material ya organizado con un propósito selectivo: distinguir entre la información disponible y retener aquella que resultó verdaderamente pertinente y útil para los objetivos del estudio, descartando lo accesorio.

En tercer lugar, la **fase de salida**, que representó el punto de llegada de todo el proceso. La información que sobrevivió los filtros de las etapas anteriores, gracias a un procedimiento de depuración riguroso y consciente, fue la que finalmente se incorpora a la investigación como insumo válido para el análisis y las conclusiones.

3.4.2. Codificación

En esta etapa, la información fue agrupada en niveles y categorías a las que se les asignó símbolos o valores numéricos derivados del desarrollo del cuestionario utilizado como instrumento de investigación.

3.4.3. Tabulación

La etapa de tabulación estuvo orientada a transformar en valores numéricos la información recabada a través de los instrumentos de recolección adoptados en este estudio, particularmente la encuesta. Gracias a este procedimiento fue posible examinar con qué regularidad se manifestaban las distintas variables contempladas en la investigación, valiéndose de escalas e intervalos previamente establecidos. De igual forma, este proceso favoreció la construcción de cuadros estadísticos y representaciones visuales de los datos de manera ordenada y comprensible, apoyándose en herramientas informáticas como Excel.

3.4.4. Registro de los datos

Esta fase comprendió la sistematización y ordenamiento de toda la información recopilada, articulándose en torno a los componentes estructurales del trabajo, entre los que se incluyen el índice general, el índice de tablas y el índice de figuras o gráficos.

3.4.5. Presentación de datos

En el marco de cualquier proceso investigativo, la exposición de los resultados demanda un tratamiento estadístico riguroso de las conclusiones e inferencias derivadas del análisis. En el presente estudio, dicha información fue organizada y presentada mediante cuadros y representaciones gráficas, tanto en su modalidad descriptiva como tabular. Este enfoque permitió visualizar los datos con mayor precisión y nivel de detalle, contribuyendo a una comprensión más integral y accesible de los hallazgos alcanzados a lo largo de la investigación.

Capítulo IV: Resultados

4.1. Análisis de resultados

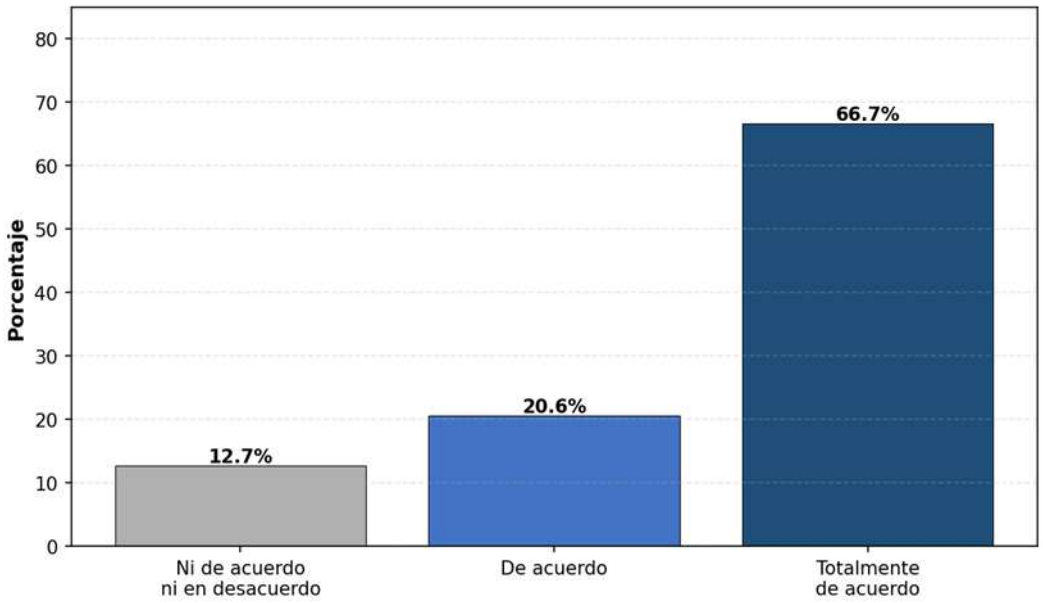
Resultado 1

¿Considera que el fraude informático en el Distrito Fiscal de Lima Centro queda impune debido a la falta de especialización técnica de los fiscales y jueces en el manejo de evidencia digital?

Tabla 4. Opinión sobre Fraude informático por falta de especialización técnica

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ni de acuerdo ni en desacuerdo	8	12.7	12.7	12.7
	De acuerdo	13	20.6	20.6	33.3
	Totalmente de acuerdo	42	66.7	66.7	100.0
	Total	63	100.0	100.0	100.0

Figura 1. Porcentaje de opinión sobre Fraude informático por falta de especialización técnica



Interpretación:

De la figura 1, que abarca la interrogante: ¿Considera que el fraude informático en el Distrito Fiscal de Lima Centro queda impune debido a la falta de especialización técnica de los fiscales y jueces en el manejo de evidencia digital?, se observa que el 12.7% de la muestra encuestada no está de acuerdo ni en desacuerdo, el 20.6% está de acuerdo y el 66.7% está totalmente de acuerdo. A partir de ello, se logra la conclusión que, con la mayoría de un 87.3% de los encuestados (que representa a 55 operadores jurídicos), se evidencia un consenso significativo respecto a la problemática planteada, lo que confirma la relevancia del problema identificado en la presente investigación.

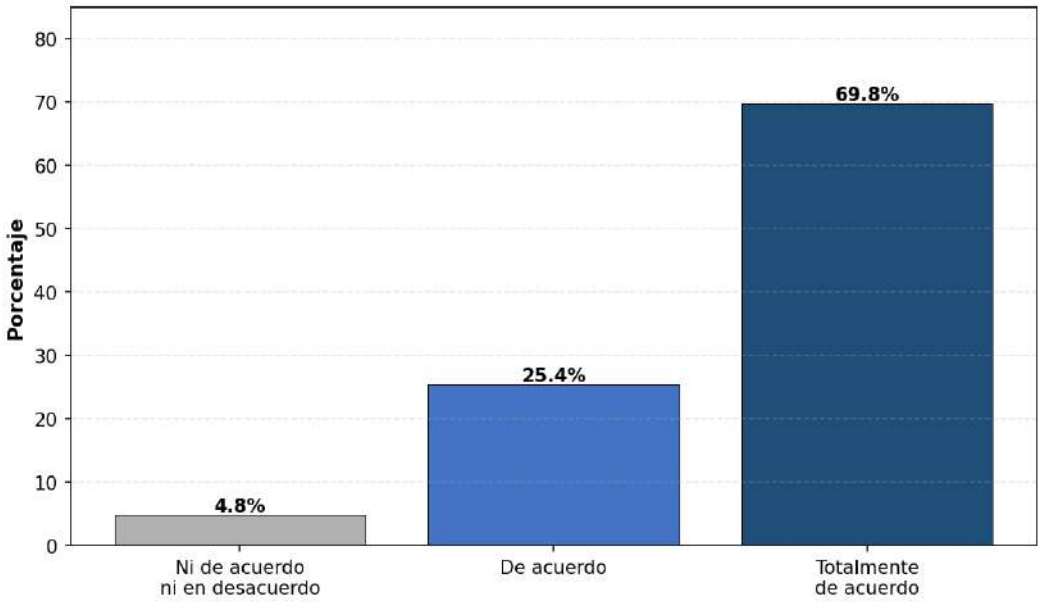
Resultado 2

¿Cree que la complejidad técnica de las transacciones digitales en casos de fraude informático dificulta la identificación de los responsables, generando altos índices de impunidad?

Tabla 5. Opinión sobre Complejidad técnica en transacciones digitales

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ni de acuerdo ni en desacuerdo	3	4.8	4.8	4.8
	De acuerdo	16	25.4	25.4	30.2
	Totalmente de acuerdo	44	69.8	69.8	100.0
	Total	63	100.0	100.0	100.0

Figura 2. Porcentaje de opinión sobre Complejidad técnica en transacciones digitales



Interpretación:

De la figura 2, que abarca la interrogante: ¿Cree que la complejidad técnica de las transacciones digitales en casos de fraude informático dificulta la identificación de los responsables, generando altos índices de impunidad?, se observa que el 4.8% de la muestra encuestada no está de acuerdo ni en desacuerdo, el 25.4% está de acuerdo y el 69.8% está totalmente de acuerdo. A partir de ello, se logra la conclusión que, con la mayoría de un 95.2% de los encuestados (que representa a 60 operadores jurídicos), se evidencia un consenso significativo respecto a la problemática planteada, lo que confirma la relevancia del problema identificado en la presente investigación.

Resultado 3

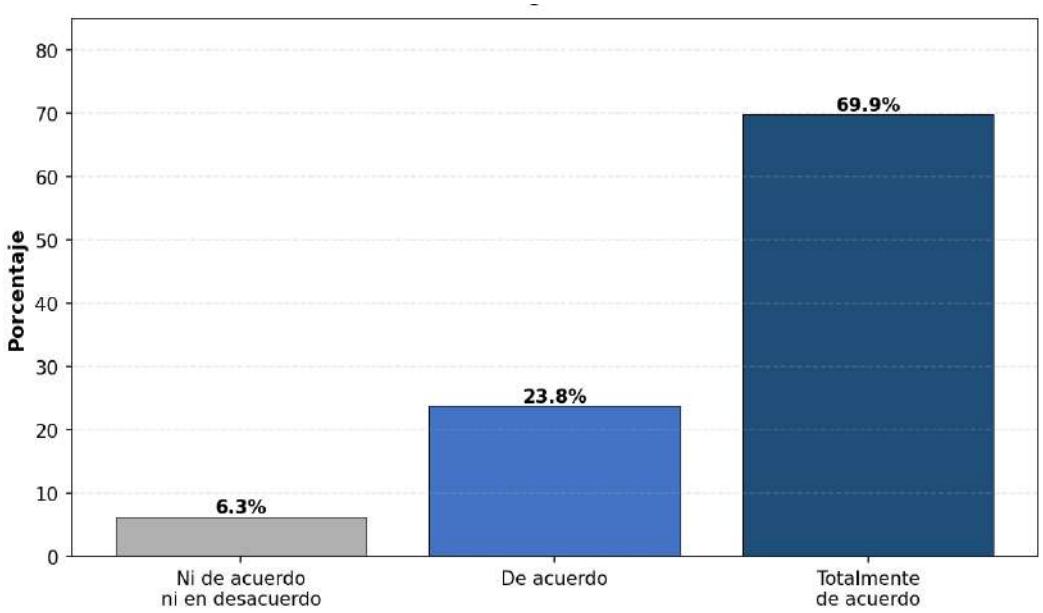
¿Considera que los casos de sabotaje informático quedan frecuentemente impunes debido a la dificultad para preservar y analizar la evidencia digital volátil?

Tabla 6. Opinión sobre Sabotaje informático y evidencia digital volátil

	Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado

Válido	Ni de acuerdo ni en desacuerdo	4	6.3	6.3	6.3
	De acuerdo	15	23.8	23.8	30.1
	Totalmente de acuerdo	44	69.9	69.9	100.0
	Total	63	100.0	100.0	100.0

Figura 3. Porcentaje de opinión sobre Sabotaje informático y evidencia digital volátil



Interpretación:

De la figura 3, que abarca la interrogante: ¿Considera que los casos de sabotaje informático quedan frecuentemente impunes debido a la dificultad para preservar y analizar la evidencia digital volátil?, se observa que el 6.3% de la muestra encuestada no está de acuerdo ni en desacuerdo, el 23.8% está de acuerdo y el 69.9% está totalmente de acuerdo. A partir de ello, se logra la conclusión que, con la mayoría de un 93.7% de los encuestados (que representa a 59 operadores jurídicos), se evidencia un consenso significativo respecto a la problemática planteada, lo que confirma la relevancia del problema identificado en la presente investigación.

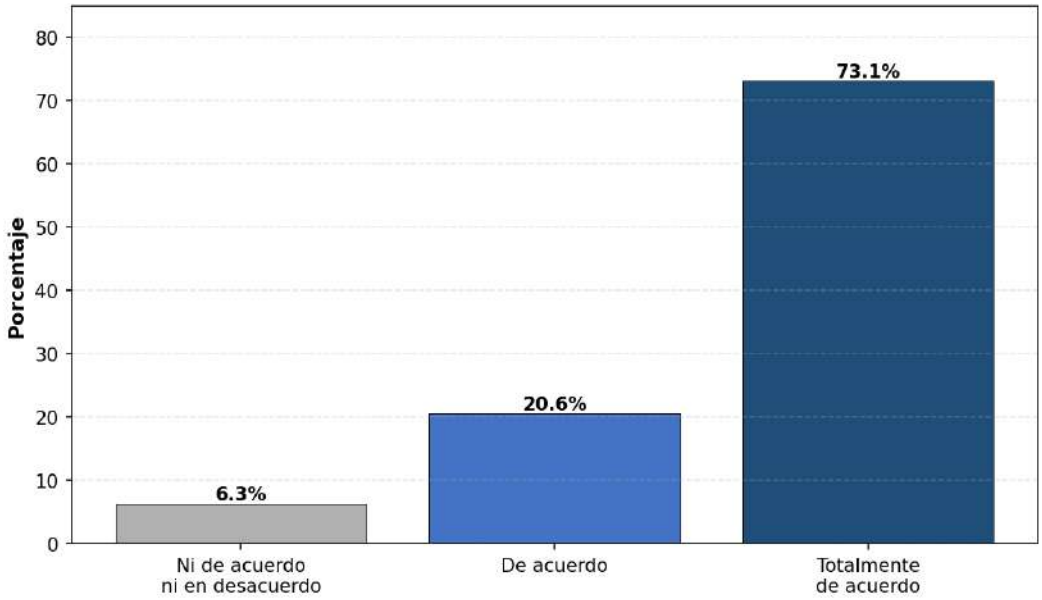
Resultado 4

¿Cree que la ausencia de peritos especializados en sistemas informáticos contribuye significativamente a la impunidad en casos de sabotaje informático?

Tabla 7. Opinión sobre Ausencia de peritos especializados

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ni de acuerdo ni en desacuerdo	4	6.3	6.3	6.3
	De acuerdo	13	20.6	20.6	26.9
	Totalmente de acuerdo	46	73.1	73.1	100.0
	Total	63	100.0	100.0	100.0

Figura 4. Porcentaje de opinión sobre Ausencia de peritos especializados



Interpretación:

De la figura 4, que abarca la interrogante: ¿Cree que la ausencia de peritos especializados en sistemas informáticos contribuye significativamente a la impunidad en casos de sabotaje informático?, se observa que el 6.3% de la muestra encuestada no está de acuerdo ni en desacuerdo, el 20.6% está de acuerdo y el 73.1% está totalmente de acuerdo. A partir de

ello, se logra la conclusión que, con la mayoría de un 93.7% de los encuestados (que representa a 59 operadores jurídicos), se evidencia un consenso significativo respecto a la problemática planteada, lo que confirma la relevancia del problema identificado en la presente investigación.

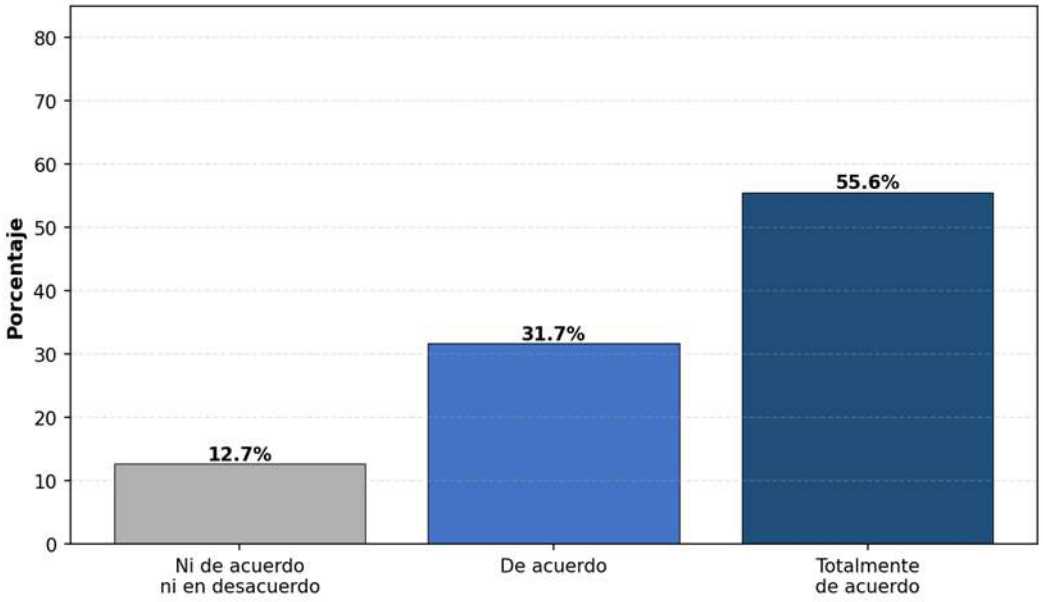
Resultado 5

¿Considera que el acceso ilícito a sistemas informáticos queda impune debido a la dificultad para rastrear el origen de los ataques cuando se emplean técnicas de anonimización?

Tabla 8. Opinión sobre Acceso ilícito y técnicas de anonimización

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ni de acuerdo ni en desacuerdo	8	12.7	12.7	12.7
	De acuerdo	20	31.7	31.7	44.4
	Totalmente de acuerdo	35	55.6	55.6	100.0
	Total	63	100.0	100.0	100.0

Figura 5. Porcentaje de opinión sobre Acceso ilícito y técnicas de anonimización



Interpretación:

De la figura 5, que abarca la interrogante: ¿Considera que el acceso ilícito a sistemas informáticos queda impune debido a la dificultad para rastrear el origen de los ataques cuando se emplean técnicas de anonimización?, se observa que el 12.7% de la muestra encuestada no está de acuerdo ni en desacuerdo, el 31.7% está de acuerdo y el 55.6% está totalmente de acuerdo. A partir de ello, se logra la conclusión que, con la mayoría de un 87.3% de los encuestados (que representa a 55 operadores jurídicos), se evidencia un consenso significativo respecto a la problemática planteada, lo que confirma la relevancia del problema identificado en la presente investigación.

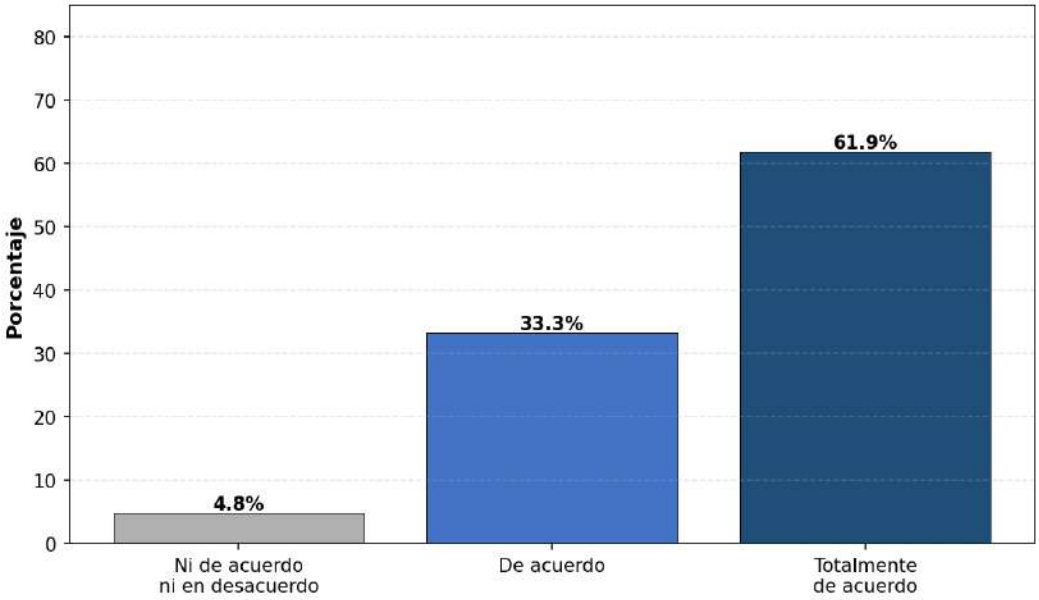
Resultado 6

¿Cree que las limitaciones técnicas de las autoridades investigadoras para identificar a los responsables de accesos ilícitos contribuyen a la impunidad de este tipo de delitos?

Tabla 9. Opinión sobre Limitaciones técnicas de autoridades investigadoras

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ni de acuerdo ni en desacuerdo	3	4.8	4.8	4.8
	De acuerdo	21	33.3	33.3	38.1
	Totalmente de acuerdo	39	61.9	61.9	100.0
	Total	63	100.0	100.0	100.0

Figura 6. Porcentaje de opinión sobre Limitaciones técnicas de autoridades investigadoras



Interpretación:

De la figura 6, que abarca la interrogante: ¿Cree que las limitaciones técnicas de las autoridades investigadoras para identificar a los responsables de accesos ilícitos contribuyen a la impunidad de este tipo de delitos?, se observa que el 4.8% de la muestra encuestada no está de acuerdo ni en desacuerdo, el 33.3% está de acuerdo y el 61.9% está totalmente de acuerdo. A partir de ello, se logra la conclusión que, con la mayoría de un 95.2% de los encuestados (que representa a 60 operadores jurídicos), se evidencia un consenso significativo respecto a la problemática planteada, lo que confirma la relevancia del problema identificado en la presente investigación.

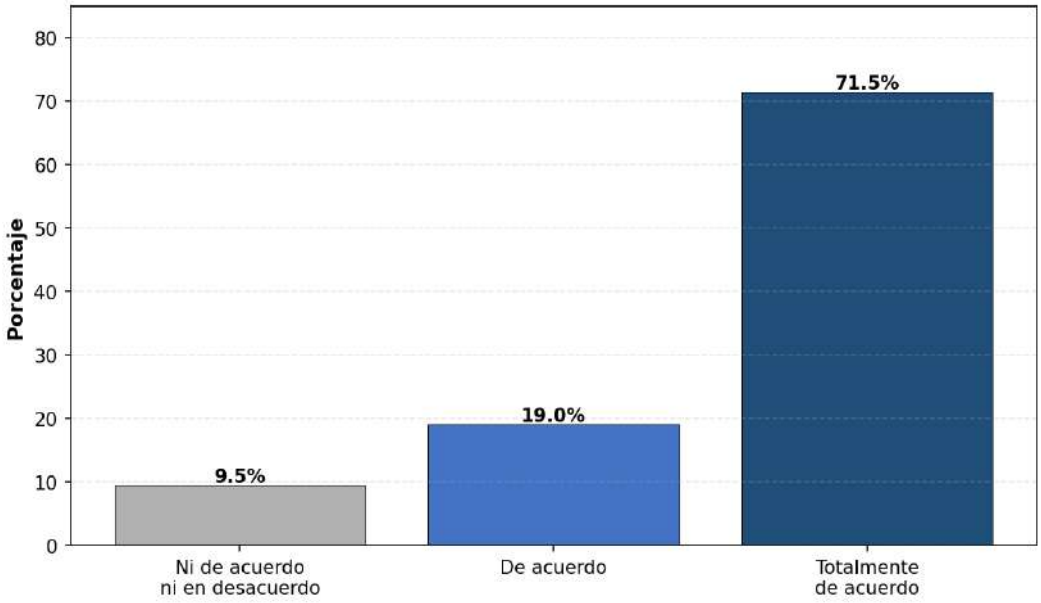
Resultado 7

¿Considera que la impunidad en delitos informáticos vulnera el derecho a la intimidad de las víctimas al no garantizarse una protección jurisdiccional efectiva frente al acceso no autorizado a su información personal?

Tabla 10. Opinión sobre Vulneración del derecho a la intimidad

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ni de acuerdo ni en desacuerdo	6	9.5	9.5	9.5
	De acuerdo	12	19.0	19.0	28.5
	Totalmente de acuerdo	45	71.5	71.5	100.0
	Total	63	100.0	100.0	100.0

Figura 7. Porcentaje de opinión sobre Vulneración del derecho a la intimidad



Interpretación:

De la figura 7, que abarca la interrogante: ¿Considera que la impunidad en delitos informáticos vulnera el derecho a la intimidad de las víctimas al no garantizarse una protección jurisdiccional efectiva frente al acceso no autorizado a su información personal?, se observa que el 9.5% de la muestra encuestada no está de acuerdo ni en desacuerdo, el 19.0% está de acuerdo y el 71.5% está totalmente de acuerdo. A partir de ello, se logra la conclusión que, con la mayoría de un 90.5% de los encuestados (que representa a 57 operadores jurídicos), se evidencia un consenso significativo respecto a la problemática planteada, lo que confirma la relevancia del problema identificado en la presente investigación.

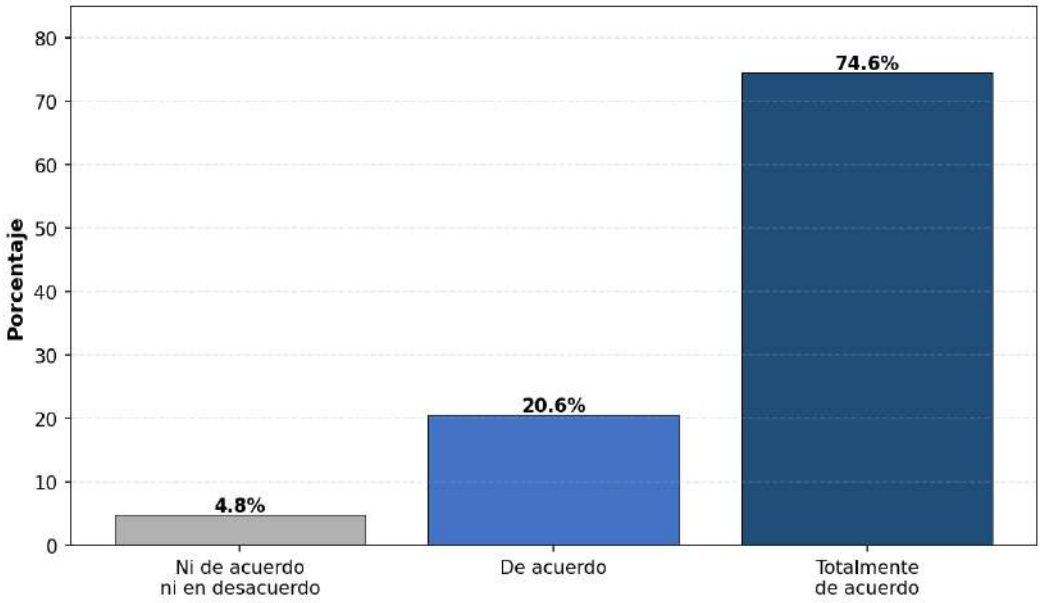
Resultado 8

¿Cree que la falta de sanciones efectivas en casos de vulneración a la intimidad mediante delitos informáticos genera inseguridad jurídica y desprotección de este derecho fundamental?

Tabla 11. Opinión sobre Inseguridad jurídica por falta de sanciones efectivas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ni de acuerdo ni en desacuerdo	3	4.8	4.8	4.8
	De acuerdo	13	20.6	20.6	25.4
	Totalmente de acuerdo	47	74.6	74.6	100.0
	Total	63	100.0	100.0	100.0

Figura 8. Porcentaje de opinión sobre Inseguridad jurídica por falta de sanciones efectivas



Interpretación:

De la figura 8, que abarca la interrogante: ¿Cree que la falta de sanciones efectivas en casos de vulneración a la intimidad mediante delitos informáticos genera inseguridad jurídica y desprotección de este derecho fundamental?, se observa que el 4.8% de la muestra

encuestada no está de acuerdo ni en desacuerdo, el 20.6% está de acuerdo y el 74.6% está totalmente de acuerdo. A partir de ello, se logra la conclusión que, con la mayoría de un 95.2% de los encuestados (que representa a 60 operadores jurídicos), se evidencia un consenso significativo respecto a la problemática planteada, lo que confirma la relevancia del problema identificado en la presente investigación.

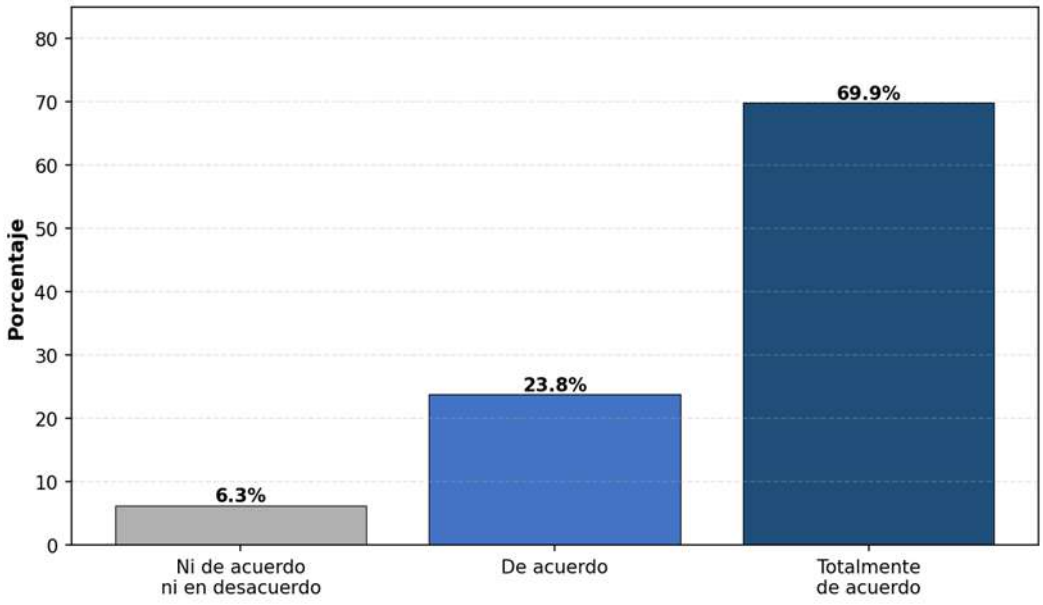
Resultado 9

¿Considera que la impunidad en casos de interceptación ilegal de comunicaciones digitales afecta gravemente el principio constitucional del secreto de las comunicaciones?

Tabla 12. Opinión sobre Interceptación ilegal de comunicaciones digitales

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ni de acuerdo ni en desacuerdo	4	6.3	6.3	6.3
	De acuerdo	15	23.8	23.8	30.1
	Totalmente de acuerdo	44	69.9	69.9	100.0
	Total	63	100.0	100.0	100.0

Figura 9. Porcentaje de opinión sobre Interceptación ilegal de comunicaciones digitales



Interpretación:

De la figura 9, que abarca la interrogante: ¿Considera que la impunidad en casos de interceptación ilegal de comunicaciones digitales afecta gravemente el principio constitucional del secreto de las comunicaciones?, se observa que el 6.3% de la muestra encuestada no está de acuerdo ni en desacuerdo, el 23.8% está de acuerdo y el 69.9% está totalmente de acuerdo. A partir de ello, se logra la conclusión que, con la mayoría de un 93.7% de los encuestados (que representa a 59 operadores jurídicos), se evidencia un consenso significativo respecto a la problemática planteada, lo que confirma la relevancia del problema identificado en la presente investigación.

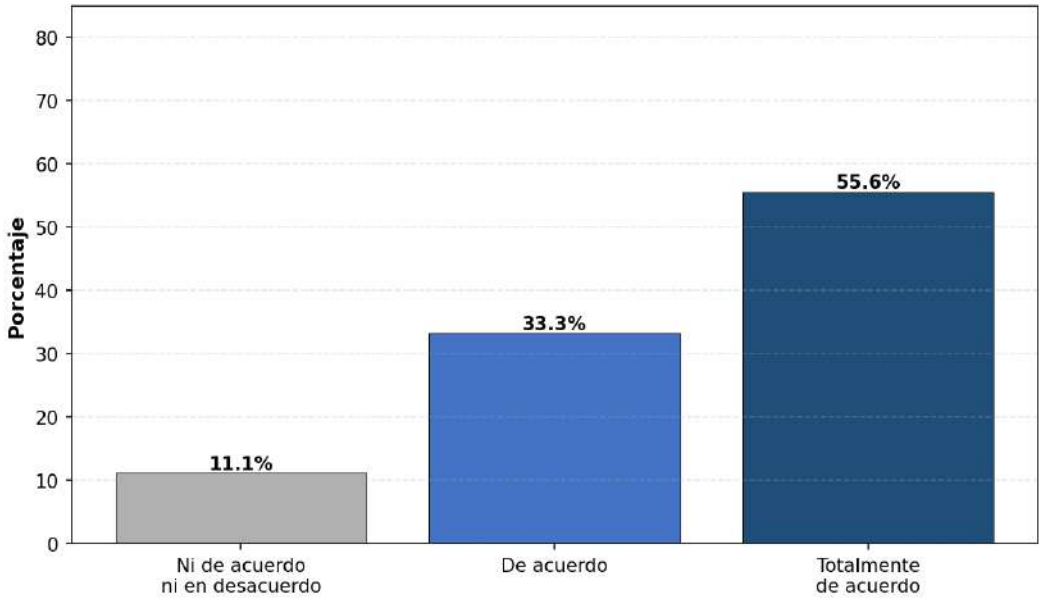
Resultado 10

¿Cree que la falta de investigación y sanción efectiva en delitos de interceptación de comunicaciones electrónicas compromete la confidencialidad constitucionalmente protegida de las comunicaciones privadas?

Tabla 13. Opinión sobre Confidencialidad de comunicaciones privadas

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ni de acuerdo ni en desacuerdo	7	11.1	11.1	11.1
	De acuerdo	21	33.3	33.3	44.4
	Totalmente de acuerdo	35	55.6	55.6	100.0
	Total	63	100.0	100.0	100.0

Figura 10. Porcentaje de opinión sobre Confidencialidad de comunicaciones privadas



Interpretación:

De la figura 10, que abarca la interrogante: ¿Cree que la falta de investigación y sanción efectiva en delitos de interceptación de comunicaciones electrónicas compromete la confidencialidad constitucionalmente protegida de las comunicaciones privadas?, se observa que el 11.1% de la muestra encuestada no está de acuerdo ni en desacuerdo, el 33.3% está de acuerdo y el 55.6% está totalmente de acuerdo. A partir de ello, se logra la conclusión que, con la mayoría de un 88.9% de los encuestados (que representa a 56 operadores jurídicos), se evidencia un consenso significativo respecto a la problemática planteada, lo que confirma la relevancia del problema identificado en la presente investigación.

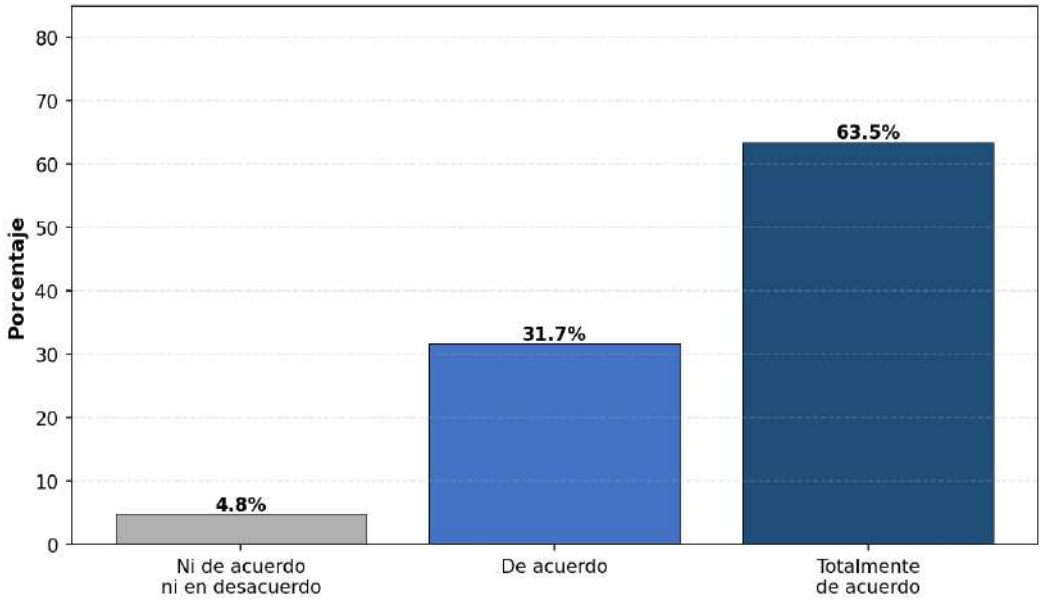
Resultado 11

¿Considera que la impunidad en delitos de sustracción y tratamiento no autorizado de datos personales vulnera el derecho fundamental a la autodeterminación informativa?

Tabla 14. Opinión sobre Autodeterminación informativa

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ni de acuerdo ni en desacuerdo	3	4.8	4.8	4.8
	De acuerdo	20	31.7	31.7	36.5
	Totalmente de acuerdo	40	63.5	63.5	100.0
	Total	63	100.0	100.0	100.0

Figura 11. Porcentaje de opinión sobre Autodeterminación informativa



Interpretación:

De la figura 11, que abarca la interrogante: ¿Considera que la impunidad en delitos de sustracción y tratamiento no autorizado de datos personales vulnera el derecho fundamental a la autodeterminación informativa?, se observa que el 4.8% de la muestra encuestada no está de acuerdo ni en desacuerdo, el 31.7% está de acuerdo y el 63.5% está totalmente de acuerdo. A partir de ello, se logra la conclusión que, con la mayoría de un 95.2% de los encuestados (que representa a 60 operadores jurídicos), se evidencia un consenso significativo respecto a la problemática planteada, lo que confirma la relevancia del problema identificado en la presente investigación.

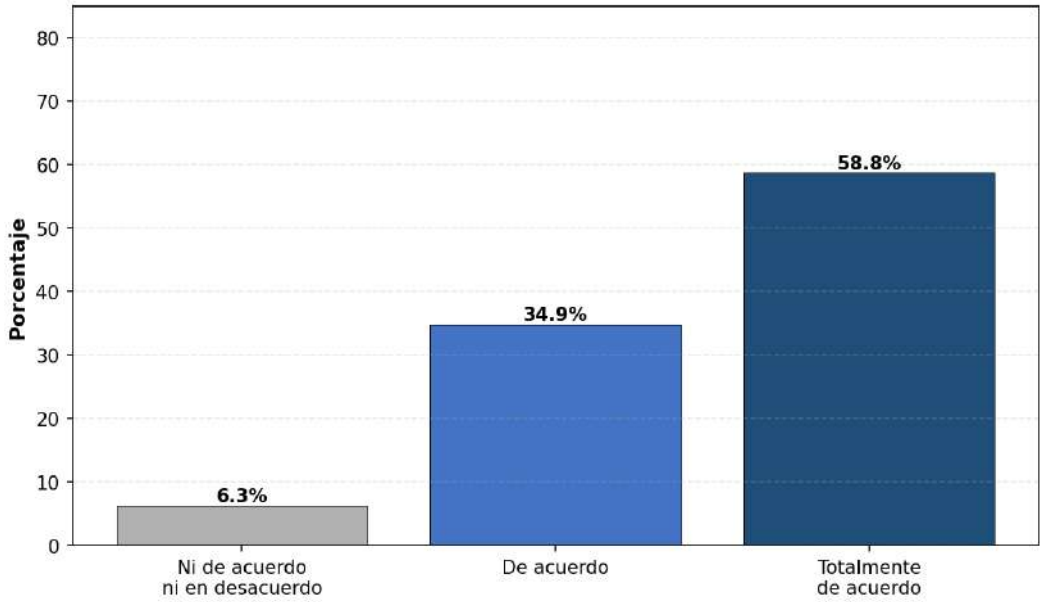
Resultado 12

¿Cree que la ausencia de respuesta penal efectiva ante vulneraciones a bases de datos personales compromete el principio constitucional de protección de datos personales establecido en la Ley N° 29733?

Tabla 15. Opinión sobre Protección de datos personales (Ley N° 29733)

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	Ni de acuerdo ni en desacuerdo	4	6.3	6.3	6.3
	De acuerdo	22	34.9	34.9	41.2
	Totalmente de acuerdo	37	58.8	58.8	100.0
	Total	63	100.0	100.0	100.0

Figura 12. Porcentaje de opinión sobre Protección de datos personales (Ley N° 29733)



Interpretación:

De la figura 12, que abarca la interrogante: ¿Cree que la ausencia de respuesta penal efectiva ante vulneraciones a bases de datos personales compromete el principio constitucional

de protección de datos personales establecido en la Ley N° 29733?, se observa que el 6.3% de la muestra encuestada no está de acuerdo ni en desacuerdo, el 34.9% está de acuerdo y el 58.8% está totalmente de acuerdo. A partir de ello, se logra la conclusión que, con la mayoría de un 93.7% de los encuestados (que representa a 59 operadores jurídicos), se evidencia un consenso significativo respecto a la problemática planteada, lo que confirma la relevancia del problema identificado en la presente investigación.

4.2. Contrastación de hipótesis

La contrastación de las hipótesis planteadas en la presente investigación se realiza tomando como parámetro fáctico, institucional y temporal de evaluación el periodo correspondiente al año 2024. Los hallazgos estadísticos obtenidos reflejan la realidad situacional del Distrito Fiscal de Lima Centro, constituyendo una línea base empírica fundamental respecto al estado de la persecución penal de los delitos informáticos con anterioridad a la vigencia y despliegue de los nuevos instrumentos de planificación digital del Estado peruano. La conjetura principal planteada en la presente investigación sostiene que la falta de sanción efectiva en materia de criminalidad informática guarda una relación significativa con la vulneración de los principios de rango constitucional en el Distrito Fiscal de Lima Centro durante el período 2024. Dicha hipótesis fue sometida a verificación a través de una interrogante específica, cuyos resultados se recogen en la décima tabla y séptima figura del análisis. La pregunta formulada buscaba determinar si la ausencia de responsabilidad penal en delitos informáticos compromete el derecho a la intimidad de las víctimas, al no garantizarse una protección jurisdiccional real frente al acceso indebido a su información personal. Los datos obtenidos mostraron que el 71.5% de los participantes expresó plena conformidad con dicha afirmación, el 19% se manifestó de acuerdo y el 9.5% adoptó una

postura intermedia. Estos hallazgos demuestran que una amplia mayoría de los operadores jurídicos del Distrito Fiscal de Lima Centro reconoce la existencia de un vínculo directo entre la impunidad en delitos informáticos y la vulneración sistemática de principios constitucionales fundamentales, lo que valida la hipótesis general formulada.

La primera hipótesis secundaria planteaba que existe una conexión significativa entre el fraude informático y la afectación de los principios constitucionales en el Distrito Fiscal de Lima Centro durante el año 2024. Esta proposición fue verificada mediante dos consultas específicas, plasmadas en la primera y segunda tabla, así como en la primera y segunda representación gráfica del análisis. La primera pregunta buscaba conocer la percepción de los encuestados respecto a si el fraude informático en dicho distrito queda sin sanción a causa de la escasa especialización técnica de fiscales y magistrados en el tratamiento de evidencia digital. Los resultados arrojaron que el 66.7% expresó total conformidad, el 20.6% señaló estar de acuerdo y el 12.7% restante adoptó una posición neutral. La segunda interrogante evaluó si la complejidad técnica de las operaciones digitales dificulta la individualización de responsables en supuestos de fraude informático, generando elevados niveles de impunidad; los resultados indicaron un 69.8% de total conformidad, un 25.4% de acuerdo y un 4.8% en posición neutral, lo que corrobora que la impunidad en esta modalidad delictiva incide directamente sobre los principios constitucionales de tutela jurisdiccional efectiva y debido proceso.

La segunda hipótesis subsidiaria proponía que la impunidad en delitos informáticos guarda una relación significativa con el sabotaje informático y su repercusión sobre los principios constitucionales en el Distrito Fiscal de Lima Centro durante el año 2024. Para su comprobación se formularon dos preguntas específicas. La primera indagaba si los casos de

sabotaje informático permanecen frecuentemente sin sanción debido a la dificultad para preservar y analizar la evidencia digital de naturaleza volátil. Los resultados se distribuyeron de la siguiente manera: el 69.9% manifestó total conformidad, el 23.8% expresó acuerdo y el 6.3% se mantuvo en una posición neutral. La segunda pregunta evaluó si la carencia de peritos especializados en sistemas informáticos contribuye de manera relevante a la impunidad en supuestos de sabotaje, obteniéndose un 73.1% de total conformidad, un 20.6% de acuerdo y un 6.3% neutral. Estos datos confirman que la falta de sanción en casos de sabotaje informático compromete seriamente los principios constitucionales de seguridad jurídica y acceso a la justicia, validando plenamente la hipótesis específica planteada.

La tercera hipótesis subordinada sostenía que la impunidad en delitos informáticos se vincula significativamente con el acceso ilícito a sistemas y su afectación sobre los principios constitucionales en el Distrito Fiscal de Lima Centro durante el año 2024. Esta proposición fue verificada a través de dos consultas específicas, recogidas en la quinta y sexta tabla, así como en la quinta y sexta figura del análisis. La primera pregunta indagaba si el acceso indebido a sistemas informáticos queda impune por la dificultad de rastrear el origen de los ataques cuando se emplean mecanismos de anonimización. Los resultados evidenciaron que el 55.6% expresó total conformidad, el 31.7% señaló estar de acuerdo y el 12.7% adoptó una posición neutral. La segunda consulta evaluó si las limitaciones técnicas de los organismos investigadores para identificar a los responsables de accesos ilícitos contribuyen a la impunidad de este tipo de conductas, obteniéndose un 61.9% de total conformidad, un 33.3% de acuerdo y un 4.8% neutral. Estos resultados demuestran que la impunidad en supuestos de acceso ilícito afecta de manera significativa los principios constitucionales de protección de datos personales, intimidad y reserva de las comunicaciones, corroborando íntegramente la

hipótesis específica formulada en la presente investigación.

Capítulo V: Discusión

Así, En relación con el fraude informático y su falta de sanción efectiva, los datos recogidos en la figura 01 revelan que la mayoría de los operadores jurídicos del Distrito Fiscal de Lima Centro, representando el 66.7% coincide plenamente en que esta modalidad delictiva permanece sin castigo a causa de la insuficiente preparación técnica de fiscales y magistrados en el tratamiento de la evidencia digital. Este hallazgo resulta concordante con las conclusiones alcanzadas por Urdanegui Rangel (2024) en su estudio titulado "Los delitos informáticos y la vulneración del derecho fundamental de protección de datos personales en Lima Metropolitana", presentado ante la Universidad Autónoma del Perú. Dicho autor sostiene que la solución adecuada a esta problemática requiere que el Estado formule una Política Nacional de Ciberseguridad, instrumento que permitiría establecer medidas preventivas integrales para evitar que más ciudadanos sean afectados por conductas de ciberdelincuencia. Al respecto, al contrastar dicha postura con el escenario institucional actual del año 2026, se advierte que si bien el Estado peruano cuenta formalmente con la Estrategia Nacional de Ciberseguridad (ESNACIB 2026-2028), nuestros datos sugieren que la dación de herramientas normativas de alta dirección gubernamental resulta insuficiente si no se abordan las deficiencias operativas de ejecución penal en las fiscalías. La criminalidad informática genera una lesión al derecho fundamental de protección de datos personales, poniendo en evidencia deficiencias estructurales en el sistema de justicia penal que comprometen la vigencia efectiva de los principios constitucionales de seguridad jurídica y tutela judicial efectiva. Esta coincidencia refuerza la urgencia de brindar formación especializada a los operadores de justicia en las áreas de criminalística digital y prueba electrónica, más allá de las declaraciones programáticas contenidas en los planes vigentes del Poder Ejecutivo.

En lo que concierne al sabotaje informático y la carencia de expertos periciales especializados, la figura 04 evidencia que el 73.1% de los operadores jurídicos del Distrito Fiscal de Lima Centro está totalmente de acuerdo en que la inexistencia de peritos con formación específica en sistemas informáticos incide de manera determinante en la falta de sanción en supuestos de sabotaje informático. Este resultado es coherente con los planteamientos de la doctrina especializada en criminalidad cibernética, en particular con lo señalado por Peña Cabrera (2015), quien advierte que la investigación y persecución de esta modalidad delictiva entraña retos de considerable complejidad, derivados de la sofisticación técnica que demanda la identificación de los métodos empleados y la atribución de responsabilidad. La impunidad en estos casos se agrava por la necesidad de contar con expertos en sistemas informáticos, las dificultades inherentes a la preservación de la evidencia digital y la exigencia de conocimientos técnicos de alto nivel para conducir las investigaciones. Esta situación compromete directamente los principios constitucionales de tutela jurisdiccional efectiva y debido proceso, en especial cuando las autoridades judiciales carecen de la especialización requerida para comprender la naturaleza técnica de estos ilícitos. Este panorama fáctico devela que la operatividad del Centro Nacional de Seguridad Digital y los lineamientos de confianza digital del país enfrentan su mayor quiebre en el eslabón de la respuesta pericial forense dentro del aparato fiscal, puesto que la volatilidad de la prueba informática sobrepasa las capacidades logísticas actuales del Ministerio Público.

Respecto a la afectación del derecho a la intimidad, los resultados de la figura 07 muestran que el 71.5% de los operadores jurídicos del Distrito Fiscal de Lima Centro considera que la impunidad en delitos informáticos lesiona el derecho a la intimidad de las víctimas, al no garantizarse una protección jurisdiccional real frente al acceso indebido a su información

personal. Este dato guarda correspondencia con lo sostenido por Landa Arroyo (2014), para quien el derecho a la intimidad en el entorno digital implica la facultad de cada persona de ejercer control sobre la información que le concierne, así como de tomar decisiones respecto a su divulgación, uso y tratamiento en espacios virtuales. La lesión a este derecho mediante conductas delictivas informáticas se manifiesta a través de diversas formas, entre ellas el acceso indebido a dispositivos personales, la obtención ilícita de información privada, la interceptación de comunicaciones electrónicas y la difusión no autorizada de datos de carácter íntimo. La ausencia de sanción en estos supuestos genera una desprotección sistemática de este derecho fundamental, creando un escenario de inseguridad jurídica en el que los ciudadanos carecen de garantías reales para salvaguardar su privacidad en el ámbito digital, afectando gravemente el libre desarrollo de la personalidad y la autonomía individual, elementos consustanciales al Estado Constitucional de Derecho. Por ende, los esfuerzos de transformación y gobernanza digital actualmente desplegados por la Presidencia del Consejo de Ministros (PCM) deben priorizar de forma obligatoria la articulación interinstitucional con los entes de persecución penal, mitigando el estado de indefensión en el que se encuentran los administrados.

Finalmente, en cuanto a la protección de datos personales y la Ley N.° 29733, la figura 12 refleja que el 58.8% de los operadores jurídicos está totalmente de acuerdo en que la ausencia de una respuesta penal eficaz frente a vulneraciones de bases de datos personales compromete el principio constitucional de protección de datos consagrado en dicha norma. Este resultado es coincidente con lo expresado por Sáenz Dávalos (2017), quien sostiene que la protección de datos personales supone el derecho de toda persona a ejercer dominio sobre su información, pudiendo decidir sobre su recopilación, tratamiento y utilización por parte de

terceros. En el contexto de los delitos informáticos, este derecho se ve gravemente menoscabado cuando los sistemas que almacenan información personal son objeto de acceso ilícito, sustracción de datos o tratamiento no consentido, sin que medie una respuesta punitiva efectiva. La falta de sanción en estos casos produce una vulneración sistemática del derecho a la autodeterminación informativa, al permitir que sujetos no autorizados accedan, utilicen y dispongan de información personal sin el consentimiento de sus titulares y sin consecuencias penales concretas, afectando así atributos esenciales como la confidencialidad, integridad y disponibilidad de los datos personales, tal como señala Remotti Carbonell (2018). Frente a ello, los datos recolectados demuestran que los retos de identidad y confianza digital planteados por la Secretaría de Gobierno y Transformación Digital no pueden consolidarse materialmente mientras persistan los elevados índices de impunidad penal detectados en las fiscalías corporativas de Lima Centro.

Capítulo VI: Conclusiones y Recomendaciones

6.1. Conclusiones

Primero: La impunidad de los delitos informáticos se relaciona significativamente con la afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024. Los resultados de la investigación evidencian que la falta de especialización técnica de los operadores de justicia, la ausencia de peritos especializados en sistemas informáticos, y las limitaciones en la preservación y análisis de evidencia digital generan altos índices de impunidad en delitos como fraude informático, sabotaje informático y acceso ilícito a sistemas. Esta impunidad compromete gravemente los principios constitucionales de tutela jurisdiccional efectiva, debido proceso, derecho a la intimidad, secreto de las comunicaciones y protección de datos personales, vulnerando la seguridad jurídica y creando un ambiente de desprotección sistemática de los derechos fundamentales de las víctimas en el ámbito digital. La investigación confirma que el 87.3% de los operadores jurídicos encuestados reconocen que existe una relación directa entre la impunidad en delitos informáticos y la vulneración de principios constitucionales fundamentales.

Segundo: El fraude informático se relaciona significativamente con la afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024. Los resultados demuestran que el 87.3% de los operadores jurídicos reconocen que la impunidad en casos de fraude informático se debe principalmente a la falta de especialización técnica de fiscales y jueces en el manejo de evidencia digital, así como a la complejidad técnica de las transacciones digitales que dificulta la identificación de los responsables. Esta situación genera una vulneración directa del principio constitucional de tutela jurisdiccional efectiva, al dejar sin protección real a las víctimas de estos delitos, comprometiendo además el derecho al debido

proceso cuando las investigaciones no se realizan con la diligencia debida o se archivan prematuramente por falta de capacidades técnicas. La impunidad en fraude informático evidencia la necesidad urgente de desarrollar capacidades institucionales especializadas que garanticen una respuesta eficaz del sistema de justicia penal.

Tercero: El sabotaje informático se relaciona significativamente con la afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024. La investigación revela que el 93.7% de los operadores jurídicos reconocen que la impunidad en casos de sabotaje informático se debe fundamentalmente a la dificultad para preservar y analizar la evidencia digital volátil y a la ausencia de peritos especializados en sistemas informáticos. Esta problemática compromete directamente los principios constitucionales de tutela jurisdiccional efectiva y debido proceso, generando situaciones donde las víctimas de sabotaje informático carecen de protección jurisdiccional real y efectiva. La naturaleza técnica de estos delitos exige una respuesta especializada del sistema de justicia que actualmente no existe, lo que perpetúa la vulneración sistemática de derechos fundamentales y debilita la confianza ciudadana en las instituciones del Estado encargadas de la persecución penal de delitos cibernéticos.

Cuarto: El acceso ilícito a sistemas informáticos se relaciona significativamente con la afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024. Los resultados evidencian que el 87.3% de los operadores jurídicos coinciden en que la impunidad en casos de acceso ilícito se genera por la dificultad para rastrear el origen de los ataques cuando se emplean técnicas de anonimización y por las limitaciones técnicas de las autoridades investigadoras. Esta impunidad afecta gravemente los principios constitucionales de protección de datos personales, derecho a la intimidad y secreto de las comunicaciones,

generando una vulneración sistemática del derecho a la autodeterminación informativa. La falta de capacidades técnicas para investigar estos delitos permite que terceros no autorizados accedan, utilicen y dispongan de información personal sin consecuencias penales efectivas, comprometiendo la confidencialidad, integridad y disponibilidad de los datos personales protegidos constitucionalmente por la Ley N° 29733.

6.2. Recomendaciones

Primero: Es fundamental que el Ministerio Público, en coordinación con el Poder Judicial y el Ministerio de Justicia y Derechos Humanos, implemente un programa integral de capacitación especializada en delitos informáticos dirigido a fiscales penales, jueces penales y personal de apoyo técnico. Este programa debe incluir módulos sobre técnicas de investigación de delitos cibernéticos, preservación y análisis de evidencia digital, manejo de herramientas forenses informáticas, y comprensión de las implicancias constitucionales de los delitos informáticos. Asimismo, se recomienda consolidación y el fortalecimiento operativo de las fiscalías y juzgados especializados en delitos informáticos en el Distrito Fiscal de Lima Centro, dotados de personal altamente capacitado y recursos tecnológicos adecuados para la investigación efectiva de estos ilícitos. Esta especialización permitirá reducir significativamente los índices de impunidad y garantizar una protección efectiva de los principios constitucionales vulnerados por la criminalidad cibernética.

Segundo: Se recomienda al Ministerio Público fortalecer el Instituto de Medicina Legal y Ciencias Forenses mediante la creación de una División Especializada en Criminalística Digital, dotada de peritos especializados en sistemas informáticos, análisis forense de dispositivos electrónicos, recuperación de datos y análisis de malware. Esta división debe contar con equipamiento tecnológico de última generación y protocolos estandarizados

para la preservación y análisis de evidencia digital, garantizando la cadena de custodia y la validez probatoria de los elementos digitales recabados en las investigaciones. Adicionalmente, se debe establecer un registro nacional de peritos especializados en informática forense que puedan ser designados como peritos de parte o peritos de oficio en investigaciones de delitos informáticos, asegurando que exista disponibilidad de experiencia técnico en todo el país para la investigación efectiva de estos delitos, articulando estas capacidades con los lineamientos técnicos fijados por el Centro Nacional de Seguridad Digital.

Tercero: El Poder Legislativo, en trabajo conjunto con el Ministerio de Justicia y Derechos Humanos, tiene la responsabilidad de promover una revisión profunda y actualizada de la Ley N.° 30096, Ley de Delitos Informáticos. Dicha reforma deberá contemplar la incorporación de nuevas figuras delictivas que respondan a las exigencias del avance tecnológico actual, la fijación de sanciones que guarden correspondencia con la entidad de los ilícitos cometidos en entornos digitales, y el diseño de procedimientos diferenciados para su investigación, preservando en todo momento las garantías constitucionales del debido proceso y la tutela jurisdiccional efectiva. En esa línea, la modificación normativa deberá incluir mecanismos concretos destinados a resguardar los derechos fundamentales de quienes resulten afectados por este tipo de conductas, con especial atención al derecho a la vida privada, la inviolabilidad de las comunicaciones y la salvaguarda de la información personal. Adicionalmente, se sugiere incorporar disposiciones que favorezcan la articulación con otros Estados en la investigación de conductas delictivas de alcance transnacional, habida cuenta de que la criminalidad en el ciberespacio no está sujeta a límites territoriales y demanda respuestas coordinadas a nivel internacional, que se complementen con el marco normativo de confianza digital del Estado peruano.

Cuarto: Se sugiere que la Presidencia del Consejo de Ministros, a través de la Secretaría de Gobierno y Transformación Digital, asuma el liderazgo en la optimización y profundización de la articulación operativa de la Estrategia Nacional de Ciberseguridad (ESNACIB 2026-2028) vigente, garantizando una integración técnica real que coordine los esfuerzos del Ministerio Público, el Poder Judicial, la Policía Nacional del Perú y demás organismos estatales con competencia en la prevención y combate de la delincuencia informática. Dicha articulación e implementación operativa deberá estructurarse en torno a los siguientes ejes fundamentales: en primer lugar, el reforzamiento de las capacidades técnicas e institucionales orientadas a la investigación de delitos cibernéticos; en segundo lugar, la elaboración de protocolos uniformes de actuación que regulen la coordinación entre las distintas entidades involucradas; en tercer lugar, el despliegue de campañas informativas dirigidas a la ciudadanía sobre los riesgos existentes en el entorno digital y las formas de proteger la información personal; en cuarto lugar, la habilitación de canales de denuncia que resulten accesibles y funcionales para las personas víctimas de este tipo de delitos; y en quinto lugar, la puesta en marcha de plataformas de información que permitan el seguimiento y la evaluación de las tendencias delictivas en el ciberespacio. En su concepción y ejecución, este plan de acción interinstitucional deberá regirse por un compromiso irrenunciable con los derechos fundamentales y los principios constitucionales, asegurando que las acciones de persecución penal no supongan en ningún caso una afectación a la privacidad, la reserva de las comunicaciones ni la protección de los datos personales de los ciudadanos.

Capítulo VII: Referencias

7.1. Referencias documentales

Defensoría del Pueblo del Perú. (2023). *Informe Defensorial sobre Ciberdelincuencia*.

Congreso de la República del Perú. (2013). *Ley N° 30096 - Ley de Delitos Informáticos*. Lima: Diario Oficial El Peruano. C.V.

Constitución Política del Perú. (1993). Lima: Congreso Constituyente Democrático.

Hernández, R. (2014). *Metodología de la investigación* (6ª ed.). Mc GRAW-HILL/ INTERAMERICANA EDITORES, S.A. DE C.V.

Real Decreto 43/2021. (2021). *Desarrollo del Real Decreto-ley 12/2018, de seguridad de las redes y sistemas de información*. BOE-A-2021-1192.

7.2. Referencias bibliográficas

Alexy, R. (2007). *Teoría de los derechos fundamentales*. Centro de Estudios Políticos y Constitucionales.

Bernales Ballesteros, E. (2012). *La Constitución de 1993: Veinte años después*. Lima: Editora Diskcopy S.A.C.

García Belaunde, D. (2016). *Manual de Derecho Constitucional*. Lima: Ediciones Legales.

García Belaunde, D. (1989). *Teoría y práctica de la Constitución peruana*. Eddili Editorial.

García Toma, V. (2003). *Valores, principios, fines e Interpretación Constitucional*. Derexho y Sociedad

García Toma, V. (2010). *Teoría del Estado y Derecho Constitucional*. Lima: Palestra Editores.

Häberle, P. (2003). *La garantía del contenido esencial de los derechos fundamentales en la Ley Fundamental de Bonn*. Dykinson.

Huerta Guerrero, L.A. (2002). *Libertad de expresión y acceso a la información pública*. Lima: Comisión Andina de Juristas.

Landa Arroyo, C. (2012). *El derecho al debido proceso en la jurisprudencia*. Lima: Academia de la Magistratura.

Landa Arroyo, C. (2014). *Los derechos fundamentales en la jurisprudencia del Tribunal Constitucional*. Lima: Palestra Editores.

Peña Cabrera, R. (2015). *Tratado de Derecho Penal. Parte Especial*. Lima: Editorial Moreno S.A.

Quiroga León, A. (2014). *Derecho Constitucional Peruano y la Constitución de 1993*. Lima: Editorial Gaceta Jurídica. Episteme.

Quiroga León, A. (2003). *El debido proceso legal en el Perú y el sistema interamericano de protección de derechos humanos*. Editorial Jurista Editores.

Remotti Carbonell, J. C. (2018). *La protección de datos personales en la jurisprudencia del Tribunal Constitucional*. Palestra Editores.

Sáenz Dávalos, L. R. (2017). *Los derechos fundamentales en la era digital*. Gaceta Jurídica.

Villavicencio Terreros, F. (2014). *Derecho Penal: Parte General*. Grijley.

7.3. Referencias hemerográficas

Estrada Salvador, C. T., & Ramirez, S. (2024). La impunidad en los delitos informáticos. Una problemática de poco interés por los legisladores, jueces y fiscales. *Revista Ius vocatio*, *7*(9).

García Toma, V. (2003). Valores, principios, fines e Interpretación Constitucional. *Derecho & Sociedad*, (21), 190-209.

Montes D. V. (2024). La vulneración del derecho a la intimidad y a la privacidad en el entorno digital en el Perú [Tesis de Licenciatura, Universidad ESAN. Facultad de Derecho y Ciencias Sociales.

Ñaupas, H., Valdivia, M., Palacios, J., & Romero, H. (2018). Metodología de la Investigación Científica - Cuantitativa - Cualitativa y Redacción de la Tesis. DGP Editores SAS. http://www.biblioteca.cij.gob.mx/Archivos/Materiales_de_consulta/Drogas_de_Abuso/Articulos/MetodologiaInvestigacionNaupas.pdf

Otzen, T., Manterola C. (2017). Técnicas de Muestreo sobre una Población a Estudio. https://www.scielo.cl/scielo.php?script=sci_arttext&pid=S0717-95022017000100037

Valdivia, M. (2018). Metodología de la investigación. Cualitativa, Cuantitativa y Redacción de Tesis (pp. 332-345). Ediciones de la U.

Villavicencio Terreros, F. (2014). Delitos Informáticos. *IUS ET VERITAS*, Revista de los estudiantes de la Facultad de Derecho de la PUCP, (49), 308-323.

7.4. Referencias electrónicas

Landa Arroyo, C. (2016). La constitucionalización del derecho administrativo. *THEMIS Revista de Derecho*, (69), 197-208. Recuperado de: https://revistas.pucp.edu.pe/index.php/themis/article/view/16725

LP Derecho. (2023). *Los principios generales del derecho administrativo*. Recuperado de: https://lpderecho.pe/principios-generales-derecho-administrativo/

LP Derecho. (2025). Ley de Delitos Informáticos (Ley 30096) [actualizada]. https://lpderecho.pe/ley-delitos-informaticos-ley-30096/

Ministerio de Justicia y Derechos Humanos. (2018). *Ley de Protección de Datos Personales - Ley N° 29733 y su Reglamento*. https://www.gob.pe/institucion/minjus/informes-publicaciones/1678029-ley-n-29733

Ministerio Público - Fiscalía de la Nación. (2014). *Ley N°30096, Ley de Delitos Informáticos y su modificatoria Ley N°30171*. https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096

PUCP. (2023). El delito de hacking o acceso ilícito a sistemas informáticos. *THEMIS Revista de Derecho*. https://revistas.pucp.edu.pe/index.php/themis/article/view/28067

UNIR Perú. (2024). ¿Qué son los delitos informáticos y qué tipos hay? https://peru.unir.net/revista/derecho/tipos-delitos-informaticos/

Universidad Continental. (2023). El principio de legalidad en el derecho administrativo. https://blogposgrado.ucontinental.edu.pe/el-principio-de-legalidad-en-el-derecho-

administrativo

Capítulo VIII: Anexos

Anexo 01: Matriz de consistencia

Título	Problema	Objetivo	Hipótesis	Variables
Impunidad de los delitos informáticos y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024	**Problema General:** ¿Qué relación tiene la impunidad de los delitos informáticos y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024? **Problemas específicos:** **Pe1:** ¿Qué relación existe entre el fraude informático y su afectación a los principios constitucionales en el Distrito Fiscal de Lima Centro, 2024? **Pe2:** ¿Qué relación existe entre el sabotaje informático y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024? **Pe3:** ¿Qué relación existe entre el acceso ilícito y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024?	**Objetivo General:** Determinar la relación que tiene la impunidad de los delitos informáticos y la afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024. **Objetivos específicos:** **Oe1:** Determinar la relación que existe entre el fraude informático y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024. **Oe2:** Determinar la relación que existe entre el sabotaje informático y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024. **Oe3**: Determinar la relación que existe entre el acceso ilícito y su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024.	**Hipótesis General:** La impunidad de los delitos informáticos se relacionaría significativamente con su afectación a los Principios constitucionales del Distrito Fiscal de Lima Centro, 2024. **Hipótesis específicas:** **He1:** El fraude informático se relacionaría significativamente con su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024. **He2:** El sabotaje informático se relacionaría significativamente con su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024. **He3:** El acceso ilícito se relacionaría significativamente con su afectación a los Principios constitucionales en el Distrito Fiscal de Lima Centro, 2024.	**Variable Independiente:** Delitos informáticos **Variable Dependiente:** Principios constitucionales

Anexo 02: Cuestionario de encuesta

ANEXO 01
CUESTIONARIO PARA ENCUESTA

"IMPUNIDAD DE LOS DELITOS INFORMÁTICOS Y SU AFECTACIÓN A LOS PRINCIPIOS CONSTITUCIONALES EN EL DISTRITO FISCAL DE LIMA CENTRO, 2024"

INSTRUCCIONES:
El presente cuestionario tiene como objetivo recopilar información sobre la impunidad de los delitos informáticos y su afectación a los principios constitucionales en el Distrito Fiscal de Lima Centro. Sus respuestas son de gran valor para nuestra investigación. Le solicitamos responder con sinceridad marcando la alternativa que mejor refleje su opinión profesional.

1. Desde su experiencia profesional, ¿Considera que el fraude informático en el Distrito Fiscal de Lima Centro queda impune debido a la falta de especialización técnica de los fiscales y jueces en el manejo de evidencia digital?
a) Ni de acuerdo ni en desacuerdo
b) De acuerdo
c) Totalmente de acuerdo

2. Según su posición profesional, ¿Cree que la complejidad técnica de las transacciones digitales en casos de fraude informático dificulta la identificación de los responsables, generando altos índices de impunidad?
a) Ni de acuerdo ni en desacuerdo
b) De acuerdo
c) Totalmente de acuerdo

3. Desde su experiencia personal, ¿Considera que los casos de sabotaje informático quedan frecuentemente impunes debido a la dificultad para preservar y analizar la evidencia digital volátil?
a) Ni de acuerdo ni en desacuerdo
b) De acuerdo
c) Totalmente de acuerdo

4. Según su perspectiva profesional, ¿Cree que la ausencia de peritos especializados en sistemas informáticos contribuye significativamente a la impunidad en casos de sabotaje informático?
a) Ni de acuerdo ni en desacuerdo
b) De acuerdo
c) Totalmente de acuerdo

5. Desde su posición profesional, ¿Considera que el acceso ilícito a sistemas informáticos queda impune debido a la dificultad para rastrear el origen de los ataques cuando se emplean técnicas de anonimización?
a) Ni de acuerdo ni en desacuerdo
b) De acuerdo
c) Totalmente de acuerdo

6. Según su experiencia personal, ¿Cree que las limitaciones técnicas de las autoridades investigadoras

para identificar a los responsables de accesos ilícitos contribuyen a la impunidad de este tipo de delitos?
a) Ni de acuerdo ni en desacuerdo
b) De acuerdo
c) Totalmente de acuerdo

7. Desde su perspectiva profesional, ¿Considera que la impunidad en delitos informáticos vulnera el derecho a la intimidad de las víctimas al no garantizarse una protección jurisdiccional efectiva frente al acceso no autorizado a su información personal?
a) Ni de acuerdo ni en desacuerdo
b) De acuerdo
c) Totalmente de acuerdo

8. Según su posición personal, ¿Cree que la falta de sanciones efectivas en casos de vulneración a la intimidad mediante delitos informáticos genera inseguridad jurídica y desprotección de este derecho fundamental?
a) Ni de acuerdo ni en desacuerdo
b) De acuerdo
c) Totalmente de acuerdo

9. Desde su experiencia profesional, ¿Considera que la impunidad en casos de interceptación ilegal de comunicaciones digitales afecta gravemente el principio constitucional del secreto de las comunicaciones?
a) Ni de acuerdo ni en desacuerdo
b) De acuerdo
c) Totalmente de acuerdo

10. Según su perspectiva personal, ¿Cree que la falta de investigación y sanción efectiva en delitos de interceptación de comunicaciones electrónicas compromete la confidencialidad constitucionalmente protegida de las comunicaciones privadas?
a) Ni de acuerdo ni en desacuerdo
b) De acuerdo
c) Totalmente de acuerdo
11. Desde su posición profesional, ¿Considera que la impunidad en delitos de sustracción y tratamiento no autorizado de datos personales vulnera el derecho fundamental a la autodeterminación informativa?
a) Ni de acuerdo ni en desacuerdo
b) De acuerdo
c) Totalmente de acuerdo

12. Según su experiencia personal, ¿Cree que la ausencia de respuesta penal efectiva ante vulneraciones a bases de datos personales compromete el principio constitucional de protección de datos personales establecido en la Ley N° 29733?
a) Ni de acuerdo ni en desacuerdo
b) De acuerdo
c) Totalmente de acuerdo