UNIVERSIDAD ANDINA

NÉSTOR CÁCERES VELÁSQUEZ

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024

TESIS PRESENTADA POR:

Bach. BLANCA LUZ CLARITA CARCAUSTO MAMANI

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADA

JULIACA – PERÚ

2025

UNIVERSIDAD ANDINA

NÉSTOR CÁCERES VELÁSQUEZ

FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

ESCUELA PROFESIONAL DE DERECHO

DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024

TESIS PRESENTADA POR:

Bach. BLANCA LUZ CLARITA CARCAUSTO MAMANI

PARA OPTAR EL TÍTULO PROFESIONAL DE:

ABOGADA

APROBADA POR EL JURADO REVISOR:

PRESIDENTE : Dr. JAVIER ROMULO QUISPE ZAPANA

PRIMER MIEMBRO : Dr. WALTHER MARCELINO NIETO PORTOCARRERO

SEGUNDO MIEMBRO : Dr. HUGO NEPTALI CAVERO AYBAR

ASESOR DE TESIS : Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO

LÍNEA DE INVESTIGACIÓN : DERECHO PÚBLICO – P05

RESOLUCIÓN Nº 00300-2025-D/FCJP-UANCV

Juliaca, 01 de diciembre de 2025.

Vistos: El expediente, **2025-C-8500** presentado por la Bachiller en Derecho **Srta. BLANCA LUZ CLARITA CARCAUSTO MAMANI**, quien solicita nominación de jurados, fecha y hora para rendir el examen de sustentación de borrador de tesis denominado: **DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024**, línea de investigación: **DERECHO PÚBLICO - P05**, para optar el Título Profesional de **ABOGADA** y;

CONSIDERANDO:

Que, de conformidad al Reglamento de Grados y Títulos de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho, concordante con el Reglamento General de Grados y Títulos de la UANCV, es procedente acceder a la petición del interesado.

Y estando, la opinión favorable del Director de la Unidad de Investigación y el Decano de la Facultad de Ciencias Jurídicas y Políticas y las atribuciones que confiere el artículo 28ª del Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos, Resolución Nª 0294-2023-UANCV-CU-R.

RESUELVE:

Primero.- **DECLARAR APTO** el informe final de la investigación (Borrador de Tesis), por tanto debe señalarse lugar, día y hora para la sustentación del borrador de tesis, en forma presencial, presentado por la Bach. **Srta. BLANCA LUZ CLARITA CARCAUSTO MAMANI**, para optar el Título Profesional de **ABOGADA**, el mismo que se llevará a cabo el próximo **miércoles, 10 de Diciembre de 2025 a las 8:00:00 AM.** lugar **FILIAL PUNO - SALON DE GRADOS JR. TACNA Nº 787**.

Segundo.- **Designar** como Jurados, para la evaluación del examen de sustentación de tesis referido, Integrado por los siguientes docentes:

Presidente del jurado : **Dr. JAVIER ROMULO QUISPE ZAPANA**

Primer miembro : **Dr. WALTHER MARCELINO NIETO PORTOCARRERO**

Segundo miembro : **Dr. HUGO NEPTALI CAVERO AYBAR**

ASESOR:

Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO

Tercero.- La Comisión de Grados y Títulos de la Facultad, Secretaria Académica y Administrativa quedan encargadas del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
DECANO
Dr. JOSÉ DOMINGO CHOQUEHUANCA CALCINA
DECANO
FAC. Cs. JURÍDICAS Y POLÍTICAS

DISTRIBUCIÓN:
DECANATURA FCJP, INTERESADO.
ARCH. FTChV/ncv.

UNIVERSIDAD ANDINA "Néstor Cáceres Velásquez"
Facultad de Ciencias Jurídicas y Políticas
UNIDAD DE INVESTIGACIÓN

RESOLUCIÓN Nº 0577-2024-UI-FCJP-UANCV-J

Juliaca, 22 de septiembre de 2025

VISTOS:

El Expediente: **2025-C-4010** de fecha **15 de septiembre de 2025**, presentado por la **Bach. BLANCA LUZ CLARITA CARCAUSTO MAMANI,** quien solicita Revisión del Informe Final de la Investigación (borrador de Tesis) y el **Anexo (04 o 05) "Ficha de Opinión del Informe Final de la Investigación (borrador de Tesis)"** que fue revisada por el Comité de Investigación de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho.

CONSIDERANDO:

Que, las Unidades de Investigación son unidades académicas que agrupan a docentes y estudiantes de diversas disciplinas, en razón del desarrollo de investigación científica, tecnológica y humanista de acuerdo al Estatuto Universitario Modificado 2020 de nuestra primera Casa Superior de Estudios.

Que, la **Bach.** BLANCA LUZ CLARITA CARCAUSTO MAMANI, quien solicita la revisión del Informe Final de la Investigación (borrador de Tesis) del tema titulado: **DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024,** línea de investigación: **DERECHO PÚBLICO - P05,** conducente para optar el Título profesional de **ABOGADA.**

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos plasmado en la Resolución Nº 0294-2023-UANCV-CU-R.

Que, el Comité de Investigación emitió su opinión favorable al Informe Final de la Investigación (borrador de Tesis).

Que, el Director de la Unidad de Investigación de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho, corroboro el asesoramiento en el Informe Final de la Investigación (borrador de Tesis) del ASESOR Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO,

Estando, la opinión favorable del comité de Investigación, en concordancia con el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos Resolución Nº 0294-2023-UANCV-CU-R, de conformidad a lo que establece la Ley Universitaria Nº 30220, Ley de Creación de la UANCV Nº 23738 y Modificatoria Nº 24661 y el Estatuto de la UANCV, que confiere facultades a la unidad de Investigación de la Facultad de Ciencias Jurídicas y Políticas.

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR Y AUTORIZAR EL INFORME FINAL DE LA INVESTIGACIÓN (BORRADOR DE TESIS) para la **REVISIÓN DE SIMILITUD TURNITIN**, del tema titulado: **DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024**, presentado por la **Bach. BLANCA LUZ CLARITA CARCAUSTO MAMANI**, para optar el Título Profesional de **ABOGADA**, en virtud de los considerandos expuestos.

ARTICULO SEGUNDO.- RATIFICAR, como ASESOR al **Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO.**

ARTICULO TERCERO.- DISPONER que la facultad, secretarias académicas y administrativas, quedan encargados del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
DECANO
Dr. JOSÉ ROBERTO RODRIGUEZ HUANCA CALCINA
DECANO
FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

UNIVERSIDAD ANDINA "NÉSTOR CÁCERES VELÁSQUEZ"
Mg. LUIS CHAVEZ AGUILAR
DIRECTOR (e)
UNIDAD DE INVESTIGACIÓN

DISTRIBUCIÓN:
ARCHIVO/CHIV.

UNIVERSIDAD ANDINA "Néstor Cáceres Velásquez"
Facultad de Ciencias Jurídicas y Políticas
UNIDAD DE INVESTIGACIÓN

DERECHO

RESOLUCIÓN Nº 0453-2025-UI-FCJP-UANCV-J

Juliaca, 26 de julio de 2025

VISTOS:

El Expediente: **2025-C-000736** de fecha **25 de julio de 2025**, el cual solicita Revisión de propuesta de Investigación y el **Anexo (02 o 03) "Ficha de Opinión de la Propuesta de Investigación"** que fue revisada por el Comité de Investigación de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho.

CONSIDERANDO:

Que, las Unidades de Investigación son unidades académicas que agrupan a docentes y estudiantes de diversas disciplinas, en razón del desarrollo de investigación científica, tecnológica y humanista de acuerdo al Estatuto Universitario Modificado 2020 de nuestra primera Casa Superior de Estudios.

Que, la **Bach.** BLANCA LUZ CLARITA CARCAUSTO MAMANI, quien solicita la revisión y aprobación de la propuesta de Investigación de **Título: DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024**, línea de investigación: **DERECHO PÚBLICO - P05**, conducente para optar el Título profesional de **ABOGADA.**

Que, al haberse cumplido con los requisitos exigidos por el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos plasmado en la Resolución Nº 0294-2023-UANCV-CU-R.

Que, el Comité de Investigación emitió su opinión favorable a la propuesta de investigación.

Que, el Director de la Unidad de Investigación de la Facultad de Ciencias Jurídicas y Políticas, Escuela Profesional de Derecho, corroboro la propuesta del ASESOR Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO, quien debe estar acreditado y facultado para orientar y ayudar al asesorado en el proceso de elaboración del trabajo de investigación (Tesis) de acuerdo a la DIRECTIVA Nº 004-2019-UANCV-VRAD-OI; y,

Estando, la opinión favorable del comité de Investigación, en concordancia con el Reglamento Interno de Trabajo de Investigación Conducente a Grados y Títulos Resolución Nº 0294-2023-UANCV-CU-R, de conformidad a lo que establece la Ley Universitaria Nº 30220, Ley de Creación de la UANCV Nº 23738 y Modificatoria Nº 24661 y el Estatuto de la UANCV, que confiere facultades a la unidad de Investigación de la Facultad de Ciencias Jurídicas y Políticas.

SE RESUELVE:

ARTICULO PRIMERO.- APROBAR Y AUTORIZAR LA EJECUCIÓN DE LA PROPUESTA DE INVESTIGACIÓN, titulado: **DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024**, presentado por la **Bach. BLANCA LUZ CLARITA CARCAUSTO MAMANI**, en virtud de los considerandos expuestos.

ARTICULO SEGUNDO.- RECONOCER, como ASESOR al **Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO.**

ARTICULO TERCERO.- DISPONER que la facultad, secretarias académicas y administrativas, quedan encargados del cumplimiento de la presente resolución.

Regístrese, comuníquese y archívese.

UNIVERSIDAD ANDINA "NESTOR CACERES VELASQUEZ"
Dr. JOSÉ DOMINGO CHOQUEHUANCA CALCINA
DECANO
FAC. Cs. JURÍDICAS Y POLÍTICAS

UNIVERSIDAD ANDINA "NESTOR CACERES VELASQUEZ"
DIRECCIÓN
JULIACA

UNIVERSIDAD ANDINA "NESTOR CACERES VELASQUEZ"
Mg. LUIS CHAYÑA AGUILAR
DIRECTOR (e)
UNIDAD DE INVESTIGACIÓN
FAC. Cs. JURÍDICAS Y POLÍTICAS

DISTRIBUCIÓN:
DECANATURA FCJP, INTERESADO.
ARCH. FTChV/ncv.

DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024

INFORME DE ORIGINALIDAD

25%	23%	14%	17%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	Submitted to Universidad Andina Nestor Caceres Velasquez Trabajo del estudiante	6%
2	hdl.handle.net Fuente de Internet	3%
3	Submitted to Universidad Privada Antenor Orrego 2025 Trabajo del estudiante	2%
4	www.informatica-juridica.com Fuente de Internet	1%
5	repositorio.caen.edu.pe Fuente de Internet	1%
6	repositorio.uancv.edu.pe Fuente de Internet	1%
7	blog.pucp.edu.pe Fuente de Internet	1%
8	repositorio.utelesup.edu.pe Fuente de Internet	<1%
9	repositorio.umet.edu.ec:8080 Fuente de Internet	<1%
10	monicasanchezminchola.blogspot.com Fuente de Internet	<1%
11	garciabelaunde.com Fuente de Internet	<1%
12	repositorio.uss.edu.pe Fuente de Internet	<1%
13	Submitted to Pontificia Universidad Catolica del Peru Trabajo del estudiante	<1%

METADATOS COMPLEMENTARIOS – UANCV

TITULO DE LA TESIS	
DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024	
Datos de autor	
Nombres y apellidos	BLANCA LUZ CLARITA CARCAUSTO MAMANI
Tipo de documento de identidad	DNI
Número de documento de identidad	73645496
URL de ORCID	https://orcid.org/0009-0004-0691-8039
Datos de asesor	
Nombres y apellidos	FELIX CRISTOBAL OCHATOMA PARAVICINO
Tipo de documento de identidad	DNI
Número de documento de identidad	02436114
URL de ORCID	https://orcid.org/0000-0003-0655-8198
Datos del jurado	
Presidente del jurado	
Nombres y apellidos	JAVIER ROMULO QUISPE ZAPANA
Tipo de documento	DNI
Número de documento de identidad	01324996
Miembro del jurado 1	
Nombres y apellidos	WALTHER MARCELINO NIETO PORTOCARRERO
Tipo de documento	DNI
Número de documento de identidad	23945399
Miembro del jurado 2	
Nombres y apellidos	HUGO NEPTALI CAVERO AYBAR
Tipo de documento	DNI
Número de documento de identidad	01332589

Datos de investigación	
Línea de investigación	DERECHO PÚBLICO - P05
Grupo de investigación	No aplica.
Agencia de financiamiento	SIN FINANCIAMIENTO
Ubicación geográfica de la investigación	**Edificio:** **País**: Perú **Departamento**: Puno **Provincia**: Puno **Distrito**: Puno **Coordenadas:** **Latitud**: -15.840008 **Longitud**: -70.020665  **URL maps:** https://maps.app.goo.gl/hxWA3X1LG61m7joZ6
Año o rango de años en que se realizó la investigación	JULIO 2025 – DICIEMBRE 2025
URL de disciplinas OCDE https://concytec-pe.github.io/Peru-CRIS/vocabularios/ocde_ford.html - Librería	**Derecho** https://concytec-pe.github.io/Peru-CRIS/vocabularios/ocde_ford.html#5.05.00 **Derecho** https://purl.org/pe-repo/ocde/ford#5.05.01

UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ
UNIDAD DE INVESTIGACIÓN
DIRECCIÓN
JULIACA - PUNO
Mg. LUIS CHAYNA AGUILAR
DIRECTOR (e)
UNIDAD DE INVESTIGACIÓN
FAC. Cs. JURÍDICAS Y POLÍTICAS

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo BLANCA LUZ CLARITA CARCAUSTO MAMANI, identificado con DNI Nro. 73645496 en mi condición de egresado de:

☒ **Escuela Profesional**

☐ **Programa de Segunda Especialidad,**

☐ **Programa de Maestría o Doctorado**

DERECHO,

informo que he elaborado el/la ☒ **Tesis** o ☐ **Trabajo de Investigación,** ☐ **Trabajo Académico** denominada:

DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024

Asesorado por: Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO

Es un tema original.

Declaro que el presente trabajo de tesis es elaborado por mi persona y **no existe plagio/copia** de ninguna naturaleza, en especial de otro documento de investigación (tesis, revista, texto, congreso, o similar) presentado por persona natural o jurídica alguna ante instituciones académicas, profesionales, de investigación o similares, en el país o en el extranjero.

Dejo constancia que las citas de otros autores han sido debidamente identificadas en el trabajo de investigación, por lo que no asumiré como suyas las opiniones vertidas por terceros, ya sea de fuentes encontradas en medios escritos, digitales o Internet.

Asimismo, ratifico que soy plenamente consciente de todo el contenido de la tesis y asumo la responsabilidad de cualquier error u omisión en el documento, así como de las connotaciones éticas y legales involucradas.

El incumplimiento de lo declarado da lugar a responsabilidad del declarante, en consecuencia; a través del presente documento asumo frente a terceros, la Universidad Andina Néstor Cáceres Velásquez y/o la Administración Pública toda responsabilidad que pueda derivarse por el trabajo final presentado. Lo señalado incluye responsabilidad pecuniaria incluido el pago de multas u otros por los daños y perjuicios que se ocasionen.

Juliaca 18 de diciembre del 2025

ASESOR

FIRMA (obligatoria)

Huella

DEDICATORIA

A los profesionales de la División de Investigación de Delitos de Alta Tecnología (DIVINDAT), cuya labor diaria inspira el compromiso con la justicia, la ética y la protección de los derechos fundamentales en el entorno digital.

Blanca Luz Clarita Carcausto Mamani

AGRADECIMIENTO

A los especialistas de la DIVINDAT–PNP, por su disposición y colaboración en la provisión de información técnica esencial para comprender la complejidad de los delitos informáticos.

A los abogados, por compartir su conocimiento y experiencia en materia de protección de datos personales y derecho digital.

Blanca Luz Clarita Carcausto Mamani

ÍNDICE GENERAL

CAPITULO IV

RESULTADOS Y DISCUSIÓN

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La presente investigación tuvo como **objetivo** general determinar la relación entre los delitos informáticos y la vulneración del derecho a la protección de datos personales en la ciudad de Puno 2024. El estudio se desarrolló bajo una **metodología** con un enfoque cuantitativo, de tipo básico, con un nivel explicativo y diseño no experimental–transversal, orientado a identificar cómo las conductas delictivas cometidas mediante medios digitales inciden en la afectación del derecho fundamental a la privacidad y seguridad de la información personal. La **población** estuvo conformada por 84 profesionales, de los cuales 38 pertenecen a la División de Investigación de Delitos de Alta Tecnología y 46 son abogados especializados en derecho informático de la ciudad de Puno. Los **resultados** mostraron que no existe una relación estadísticamente significativa entre las variables estudiadas. Sin embargo, desde una perspectiva descriptiva, se observó que los delitos informáticos más frecuentes como el fraude electrónico, el acceso ilícito a sistemas informáticos y la suplantación de identidad digital continúan generando riesgos elevados para la protección de los datos personales reconocidos en el artículo 2, inciso 6, de la Constitución Política del Perú y en la Ley N.º 29733. Se llego a la **conclusión** que, aunque la prueba estadística no mostró correlación significativa, la presencia recurrente de ciberataques y la debilidad de las medidas de seguridad reflejan una asociación práctica y socialmente relevante entre la comisión de delitos informáticos y la vulneración de los derechos de protección de datos, lo que exige fortalecer la legislación, los mecanismos de ciberseguridad y la capacitación especializada de los operadores jurídicos y técnicos en materia de delitos tecnológicos.

Palabras claves. Delito informático, vulneración, derecho a la protección de datos personales, informáticos

ABSTRACT

The general objective of this research was to determine the relationship between cybercrimes and violations of the right to personal data protection in the city of Puno during 2024. The study was conducted using a quantitative, basic, correlational, and non-experimental cross-sectional design, aimed at analyzing how criminal acts committed through digital means affect the fundamental right to privacy and security of personal information. The population consisted of 84 professionals, 38 of whom belong to the High-Tech Crime Investigation Division and 46 of whom are lawyers specializing in computer law in the city of Puno. The results showed no statistically significant relationship between the variables analyzed. However, from a descriptive perspective, it was observed that the most frequent cybercrimes, such as electronic fraud, unauthorized access to computer systems, and digital identity theft, continue to generate high risks for the protection of personal data, as recognized in Article 2, paragraph 6, of the Political Constitution of Peru and in Law No. 29733. It was concluded that, although the statistical test did not show a significant correlation, the recurring presence of cyberattacks and the weakness of security measures reflect a practical and socially relevant association between the commission of cybercrimes and the violation of data protection rights. This necessitates strengthening legislation, cybersecurity mechanisms, and specialized training for legal and technical professionals in the field of technology-related crimes.

Keywords: Cybercrime, violation, right to personal data protection, computer crimes

INTRODUCCIÓN

En un mundo cada vez más interconectado, la información personal circula a la velocidad de un clic y los datos que ayer parecían inofensivos hoy pueden convertirse en armas silenciosas contra la intimidad y la libertad. Desde que la Convención de Budapest sobre la Ciberdelincuencia entró en vigor, los Estados comenzaron a reconocer que los delitos informáticos no eran simples incidencias técnicas, sino agresiones contra el tejido social y los derechos humanos que requerían respuestas sólidas y coordinadas. Mientras Europa refinaba su régimen de protección con el Reglamento (UE) 2016/679 marcando un estándar mundial sobre el tratamiento de datos personales, en América Latina emergía una nueva urgencia: adaptar las leyes, fortalecer la fiscalización y educar a los ciudadanos para no quedar indefensos ante la digitalización creciente.

En el Perú, ese desafío fue asumido mediante la Ley N°29733 – Ley de Protección de Datos Personales, que declaró el tratamiento de información personal como un derecho fundamental; y con la Ley Nº30096 – Ley de Delitos Informáticos, que tipificó conductas delictivas específicas vinculadas a sistemas y datos informáticos, reconociendo que la vulnerabilidad digital era hoy terreno fértil para la comisión de ilícitos. Sin embargo, lejos de la capital y de las grandes ciudades, en la región de Puno el ecosistema digital ha evolucionado sin ser completamente acompañado por la infraestructura normativa, técnica y cultural que lo proteja. Según estudios recientes, en la ciudad de Puno se advierte un crecimiento alarmante de denuncias por fraude informático, provocado por la combinación de desinformación, brechas en seguridad informática y escasa conciencia ciudadana frente a la protección de sus datos. (Ticona, 2024)

Esta realidad puneña, en apariencia distante del fragor de la ciberseguridad urbana encierra, sin embargo, un veredicto contundente: la digitalización no es garantía de inclusión si no viene acompañada de garantías; los riesgos no se diluyen por geografía; y la fragilidad

de los controles localizados multiplica el daño cuando la información personal es objeto de acceso no autorizado, suplantación, difamación o comercialización clandestina. En Puno, usuarios, microempresas, entidades públicas y privadas convivientes con redes sociales, plataformas de comercio electrónico y sistemas de gestión de datos enfrentan una paradoja: disponen de más conectividad, pero con menos protección. Esta disonancia genera un caldo de cultivo para los delitos informáticos que vulneran la dignidad individual al borrar los límites entre lo público y lo privado, y al debilitar los cimientos del derecho a la protección de datos personales.

La presente investigación bajo el título "Delitos informáticos y su incidencia en la vulneración del derecho a la protección de datos personales, ciudad de Puno 2024" se inscribe en ese contexto crítico. Su propósito no es solo describir un fenómeno técnico, sino revelar cómo la comisión de ilícitos digitales compromete derechos, erosiona la confianza ciudadana y desafía la capacidad del sistema penal y administrativo para responder. Al articular la dimensión internacional, nacional y local, esta tesis aspira a mostrar que la gobernanza de datos ya no es un reto exclusivo de grandes urbes o corporaciones; es una exigencia para regiones como Puno, que deben traducir los tratados y leyes en mecanismos operativos, cultura de protección y vigilancia activa para evitar que los cibercriminales sigan encontrando en la laguna normativa y técnica un territorio libre para actuar.

En efecto, la seguridad de los datos personales, la integridad de los sistemas y la eficacia penal se configuran como tres vértices inseparables de una misma problemática. Y es en ese triángulo donde se juega la legítima expectativa de que la información que compartimos, ya sea al registrarnos en una plataforma, al efectuar un pago electrónico o al declarar un dato personal esté protegida de la intrusión, el daño o el uso arbitrario. Por lo tanto, este estudio no solo diagnostica fallas normativas o técnicas, sino que propone una reflexión y una ruta que involucran a todos los actores: ciudadanos, empresas, entidades públicas, operadores de

justicia y diseño institucional. Solo así la ciudad de Puno podrá transformar la conectividad en garantía de derechos, y la tecnología no en una vía de victimización silenciosa.

La estructura del trabajo se compone de cinco capítulos detallados a continuación:

Capítulo I: Planteamiento del problema

Aquí se describe el fenómeno de los delitos informáticos y el derecho a la protección de datos personales, se fundamenta su trascendencia jurídica y social, se formula el problema de investigación, se justifica su estudio, se presentan las hipótesis, se identifican las variables y se define su operacionalización.

Capítulo II: Marco teórico y antecedentes

En este capítulo se revisan los antecedentes nacionales y locales sobre delitos en internet y la vulneración de la protección de datos personales, se desarrollan las bases teóricas (tipificación legal del delito, así como el principio de consentimiento y autodeterminación informativa) y se precisan los conceptos esenciales.

Capítulo III: Metodología de la investigación

Este capítulo expone el paradigma adoptado, el método, el nivel y diseño de estudio, así como la población, muestra, técnica e instrumentos de recolección de datos. Además, se detalla el procedimiento del trabajo de campo y la forma de análisis de los datos.

Capítulo V: Resultados, discusión y conclusiones

Finalmente, en este apartado se presentan los hallazgos de la investigación, se realiza la contrastación de las hipótesis, se discuten los resultados en relación con la teoría y normativa, y se formulan conclusiones y recomendaciones para la ciudadanía y el estado.

De esta forma, el estudio aporta una mirada jurídica-normativa y empírica sobre cómo la tipificación y regulación efectiva de los delitos informáticos inciden en la garantía y protección del derecho fundamental a la privacidad y a los datos personales, en un contexto local particularmente significativo como la ciudad de Puno, donde la expansión digital y las

brechas en ciberseguridad revelan los desafíos del sistema jurídico para resguardar la información y la dignidad de sus ciudadanos.

CAPÍTULO I

FORMULACIÓN DEL PROBLEMA

1.1. Exposición de la situación problemática

En el mundo contemporáneo, la expansión veloz de las tecnologías de la información ha propiciado un escenario en el cual los delitos informáticos adquieren una magnitud global, reduciendo los límites físicos y multiplicando las oportunidades para vulnerar derechos fundamentales como el de la protección de datos personales. En 2024, los daños económicos derivados de la ciberdelincuencia se estiman en torno a US$ 9,5 billones, cifra que sitúa al fenómeno como la tercera mayor economía ilícita del planeta. Las herramientas de ataque evolucionan, los colectivos criminales se sofisticaron y la normativa internacional lucha por ponerse al día. Desde la perspectiva jurídica, esta realidad exige revisar cómo los marcos legales y los principios de autodeterminación informativa se confrontan con un entorno dinámico y complejo. Así, emerge la necesidad de comprender no sólo la existencia del delito informático, sino su incidencia concreta sobre el derecho a la protección de datos personales en un ámbito transnacional.

En el Perú, esta problemática cobra rasgos específicos y urgentes. Un informe reciente de la Defensoría del Pueblo advierte que la ciberdelincuencia ha presentado un crecimiento notable y plantea retos significativos para el Estado en sus estrategias

de prevención e investigación. A nivel normativo, aunque existe la Ley N.º 30096 – Ley de Delitos Informáticos y la Ley Nº29733 – Ley de Protección de Datos Personales, la aplicación práctica demuestra insuficiencias en cuanto a la capacidad técnica de las instituciones, la detección de conductas ilícitas digitales y la tutela efectiva de los titulares de datos. En ese contexto, la relación entre las modalidades de delitos informáticos y la vulneración del derecho a la protección de datos personales presenta vacíos de conocimiento relevantes, especialmente en cuanto a la percepción institucional, las medidas de seguridad y la eficacia normativa.

En el ámbito local de la ciudad de Puno, la situación adquiere una dimensión aún más crítica y requiere atención específica. Aquí, el fenómeno se manifiesta entre entidades públicas y privadas que gestionan datos personales y enfrentan el aumento de delitos informáticos sin contar con protocolos robustos, mecanismos de denuncia eficaces o cultura de protección de datos consolidada. La investigación descriptiva-correlacional adoptada permite visibilizar esas carencias al medir la frecuencia subjetiva de la percepción sobre delitos informáticos y la vulneración del derecho a la protección de datos personales en Puno, durante 2021-2022. Al hacerlo, se genera evidencia localizable que puede sustentar políticas, fortalecer la gestión institucional y cerrar la brecha entre la normativa vigente y su implementación práctica en contextos regionales.

1.1.1. Problema general

PG: ¿Cómo los delitos informáticos inciden en la vulneración del derecho a la protección de datos personales, ciudad de Puno 2024?

1.1.2. Problemas especificas

- **PE1:** ¿Cómo se manifiestan los tipos más frecuentes de delitos informáticos, ciudad de Puno 2024?

- **PE2:** ¿De qué manera las medidas de seguridad y resguardo de datos inciden en la protección de la información personal, ciudad de Puno 2024?

1.2.Justificación de la investigación

1.2.1. Teórica

El alza de los delitos informáticos exige una revisión urgente del entramado teórico que sustenta la protección de los datos personales. En el orden jurídico peruano coexisten la Ley N.º 30096 (Delitos Informáticos) y la Ley N.º 29733 (Protección de Datos Personales), pero la literatura revela una carencia sustancial de estudios que integren ambas perspectivas en un diseño de tipo descriptivo correlacional en el ámbito local. Al adoptar el marco conceptual que vincula la autodeterminación informativa, los principios de seguridad y la responsabilidad penal-administrativa, esta investigación profundiza en el corpus académico existente, al aportar evidencia empírica contextualizada y al poner en tensión los supuestos normativos frente a la operatividad institucional. De ese modo, contribuye al desarrollo teórico interdisciplinario entre derecho penal informático, protección de datos y políticas públicas digitales.

1.2.2. Práctica

La creciente incidencia de vulneraciones al derecho a la protección de datos personales mediante delitos informáticos configura un problema tangible que socava la confianza ciudadana, la operatividad institucional y la vigencia de garantías fundamentales. Esta investigación cobija una utilidad concreta al materializar datos cuantitativos sobre percepción, medidas de seguridad y eficacia normativa en la ciudad de Puno, lo que permite diseñar recomendaciones de política pública ajustadas a la realidad local. Las instituciones involucradas públicas y privadas pueden utilizar los resultados como insumo para implementar estrategias de prevención, protocolos

de respuesta y capacitación especializada. Así, el estudio trasciende el plano descriptivo para generar impactos reales en la gestión institucional y en la protección jurídica de los titulares de datos.

1.2.3. Metodológica

Se ha optado por un enfoque cuantitativo, nivel descriptivo, de tipo básico y diseño no experimental transversal, debido a su idoneidad para medir con rigor la fuerza y dirección del vínculo entre los factores jurídicos y organizativos en el ámbito de los delitos informáticos y la vulneración de datos personales. Mediante encuestas precodificadas que permiten la recolección de datos numéricos fiables, esta estrategia facilita análisis estadísticos de correlación, asegurando objetividad y reproducibilidad en la medición. Al abstenerse de manipular variables y observar el fenómeno en su contexto natural, la metodología preserva la integridad del estudio, habilitando conclusiones fundamentadas y generalizables en el marco local.

1.3. Objetivos de la investigación

1.3.1. Objetivo general

Describir la incidencia de los delitos informáticos en la vulneración del derecho a la protección de datos personales, ciudad de Puno 2024.

1.3.2. Objetivo específico

- **OE1:** Identificar los tipos más frecuentes de delitos informáticos ocurridos, ciudad de Puno 2024.
- **OE2:** Examinar las medidas de seguridad y resguardo de datos personales aplicadas, ciudad de Puno 2024.

1.4.Hipótesis

1.4.1. Hipótesis general

Los delitos informáticos inciden de manera significativa en la vulneración del derecho a la protección de datos personales, ciudad de Puno 2024.

1.4.2. Hipótesis específicas

- **HE1:** Los tipos más frecuentes de delitos informáticos registrados se relacionan con incidentes de acceso ilícito y robo de identidad, ciudad de Puno 2024.
- **HE2:** La insuficiente implementación de medidas de seguridad incrementa el riesgo de vulneración del derecho a la protección de datos personales, ciudad de Puno 2024.

1.5.Variables

1.5.1. Variable independiente

Delitos informáticos.

1.5.2. Variable dependiente

Derecho a la protección de datos personales.

1.6.Operacionalización de variables

Tabla 1

Operacionalización de variables

VARIABLES	DIMENSIONES	INDICADORES
1. Delitos informáticos	1.1. Tipificación legal del delito informático	1.1.1. Hechos descritos que constituyen delitos según la Ley N.º 30096 (Delitos Informáticos)
		1.1.2. Existencia de conducta dolosa o culposa tipificada
		1.1.3. Correspondencia entre conducta y tipo penal aplicable
	1.2. Modalidad de ejecución del delito	1.2.1. Uso de medios tecnológicos para vulnerar sistemas o redes informáticas
		1.2.2. Utilización de mecanismos de suplantación o fraude digital
		1.2.3. Acceso, interceptación o alteración no autorizada de datos personales
	1.3. Responsabilidad y efectos jurídicos	1.3.1. Identificación de sujetos activos y pasivos involucrados en delitos informáticos
		1.3.2. Existencia de daño digital, patrimonial o reputacional derivado del hecho delictivo
		1.3.3. Existencia de denuncia o proceso penal en curso vinculado a cibercrimen
2. Derecho a la protección de datos personales	2.1. Principio de consentimiento y autodeterminación informativa	2.1.1. Existencia de consentimiento previo, libre y expreso del titular (Ley N.º 29733, art. 12)
		2.1.2. Registro documental del consentimiento otorgado
		2.1.3. Información clara sobre fines, uso y tratamiento de los datos personales
	2.2. Principio de seguridad y confidencialidad	2.2.1. Existencia de medidas técnicas y organizativas para la protección de datos personales (Reglamento, arts. 28–32)
		2.2.2. Existencia de protocolos de acceso, resguardo y manejo de información confidencial
		2.2.3. Realización de auditorías o controles internos en materia de ciberseguridad
	2.3. Vulneración y consecuencias jurídicas	2.3.1. Exposición, filtración o comercialización no autorizada de datos personales
		2.3.2. Afectación a la privacidad, honra o identidad digital del titular
		2.3.3. Registro de denuncias ante la Autoridad Nacional de Protección de Datos Personales o el Ministerio Público

Nota: la tabla muestra la operacionalización de variables, ejecutado por la tesista.

CAPITULO II

MARCO TEÓRICO

2.1. Antecedentes del estudio

2.1.1. A Nivel Internacional

La tesis presentada por Echeverría y Salvador (2024), una revisión sistemática, artículo del Colegio de Ingenieros en Informática de Sistemas y Computación de El Oro y Universidad Católica de Cuenca, cuyo objetivo fue analizar las técnicas y herramientas forenses más utilizadas en la investigación de delitos informáticos, simultáneamente examinando sus aspectos legales relativos a la admisibilidad de las pruebas digitales. La metodología correlacional, fundamentada en la exhaustividad de una revisión sistemática cualitativa, permitió identificar brechas legales y operativas en la lucha contra estos crímenes que vulneran el derecho a la protección de datos personales y la privacidad. Por consiguiente, la investigación reveló la magnitud global del problema: el costo de los delitos cibernéticos en 2022 alcanzó los 6 billones de dólares, lo que representa un incremento del 15% respecto a 2021. A la luz de estos datos, se constató que Ecuador experimentó un aumento del 30% en las denuncias de delitos informáticos durante 2022, evidenciando la urgente necesidad de capacitación forense y marcos legales más específicos para abordar la Revelación ilegal de bases de datos y otros atentados contra la privacidad.

Por otro lado, la tesis presentada por Sarmiento y Maldonado (2024), artículo de la Universidad Internacional del Ecuador-Uide, cuyo objetivo fue realizar un análisis profundo, tanto normativo como doctrinario, para determinar si la protección legal ecuatoriana resultaba eficaz frente a los delitos informáticos contemporáneos. La metodología correlacional, implementando un enfoque cuantitativo a través de encuestas directas a la población, subrayó la brecha existente entre la ley y el conocimiento ciudadano, un factor que agrava la incidencia de estos delitos. En efecto, los resultados mostraron que el desconocimiento sobre la vulneración de datos es alarmante: el 85.7% de los encuestados (60 de 70 personas) ignoraba que filtrar contenido íntimo conlleva penas de prisión, un delito que atenta directamente contra la intimidad y la dignidad humana. Además, la acumulación de 3.183 delitos informáticos registrados entre 2020 y 2022 exige una mayor educación y concienciación, máxime cuando la violación a la intimidad, tipificada en el Art. 178 del COIP, ha derivado en consecuencias trágicas, incluyendo reportes de suicidios.

Finalmente, la tesis presentada por Intriago y Chancay (2024), artículo de la Universidad Técnica de Manabí, Ciencias Informáticas, Portoviejo, Ecuador, cuyo objetivo fue recopilar y analizar información crucial sobre las estrategias de computación empleadas para combatir y prevenir la creciente ola de delitos informáticos en América Latina y España. La metodología correlacional, empleada en una rigurosa revisión sistemática basada en el protocolo PRISMA, permitió catalogar la diversidad de enfoques necesarios para proteger los sistemas de información personal. De manera específica, la distribución de los 24 estudios analizados reveló que las estrategias de defensa técnica son prioritarias en la región: el 52.63% de los artículos se enfocaron en técnicas de prevención, destacando que el 42% de estos se concentraron en la categoría de Detección y Prevención Técnica.

Consiguientemente, se hace evidente la necesidad de implementar soluciones avanzadas de Machine Learning e Inteligencia Artificial, tal como se observa en los enfoques punteros de España, para contrarrestar ciberataques sofisticados que buscan la vulneración de datos, como el phishing en redes Blockchain, y así mejorar la eficacia de las medidas de protección de la información.

2.1.2. A Nivel Nacional

La tesis presentada por Quincho et al. (2025), tesis de la Facultad De Derecho de la Escuela Académico Profesional de Derecho, cuyo objetivo fue contrastar la aplicación del Convenio de Budapest con respecto a la Ley de Delitos Informáticos del Perú (Ley N° 30096) para enfrentar la ciberdelincuencia. A pesar de que la investigación original utilizó un enfoque mixto para el análisis de expertos legales, la metodología correlacional se presenta como clave para vincular la rigidez normativa peruana con la incidencia criminal en la protección de datos personales. Los hallazgos subrayaron una debilidad legislativa crítica frente a los estándares internacionales. Particularmente revelador fue el dato de que el 93% de los especialistas consultados identificó vacíos en la legislación peruana con respecto al fraude informático. Asimismo, y de manera contundente, el 73% señaló deficiencias en la ley nacional en la protección contra la suplantación de identidad. Esta brecha normativa, reflejada en estos altos porcentajes, incide directamente en la vulneración de los datos personales en Perú, instando a una reforma integral.

En lo que respecta a Portugal (2024), tesis de la Universidad Privada San Carlos, cuyo objetivo fue analizar cómo la admisión de la evidencia digital incide en los delitos informáticos en el proceso penal peruano. Aun cuando su diseño se centró en un enfoque cualitativo descriptivo basado en entrevistas, la metodología correlacional podría relacionar la carencia logística policial en Puno con el problema

de la impunidad ante crímenes que vulneran la información privada. Los resultados obtenidos mediante entrevistas a efectivos policiales de Puno revelan un desafío logístico fundamental para la persecución del cibercrimen en el sur de Perú. Por consiguiente, la mayoría de los entrevistados declaró que no se posee el conocimiento adecuado ni la capacitación suficiente para el manejo y recolección de evidencia digital. Ante esta realidad, la efectividad del sistema para establecer la responsabilidad penal, a pesar de que la prueba digital se acepta generalmente como medio válido, se ve comprometida, lo que indirectamente aumenta la incidencia de la vulneración de datos personales en la región.

Por otro lado a nivel nacional, la tesis presentada por Rojas (2024), tesis de la Facultad de derecho y ciencias políticas, cuyo objetivo fue analizar la necesidad de regular nuevas modalidades del delito de fraude informático, especialmente el phishing y el uso indebido de tarjetas bancarias de terceros, frente a la creciente ciberdelincuencia en Perú. En virtud de la rápida evolución de las amenazas, la metodología correlacional se emplea para trazar el vínculo entre la insuficiencia legislativa y el aprovechamiento de tecnologías emergentes como la inteligencia artificial para el fraude. Los hallazgos revelaron que la ciberdelincuencia contra el patrimonio ha experimentado un crecimiento alarmante en Perú. A modo de ejemplo, las denuncias por Fraude Informático alcanzaron las 11,768 en 2021, marcando un aumento del 117.1% en comparación con el año anterior. Además, durante el primer trimestre de 2023, esta modalidad constituyó el 73.30% de las denuncias por delitos cibernéticos contra el patrimonio. Ante esta ola de incidentes que comprometen la información personal, la investigación concluye que es fundamental legislar sobre el phishing de manera autónoma para evitar la impunidad.

2.1.3.A nivel local

La tesis presentada por Mamanihanco (2025), tesis de la Universidad Privada San Carlos, cuyo objetivo fue determinar la eficacia de la protección de los derechos fundamentales de menores y adolescentes en redes sociales, poniendo especial énfasis en la tutela administrativa para resguardar sus datos personales en el entorno digital de Puno. No obstante, la aproximación analítico-dogmática realizada a abogados especialistas en la ciudad, la metodología correlacional se sugiere como un camino complementario para dimensionar la incidencia directa entre la desactualización normativa y la creciente vulnerabilidad digital de los jóvenes puneños. Seguidamente, este estudio identificó que la protección vigente resulta insuficiente, lo que deja a los menores expuestos a riesgos como la afectación a la intimidad y el uso indebido de sus datos personales. Consecuentemente, el consenso entre los expertos de Puno determinó una insuficiencia del marco legal, especialmente cuando se considera que el 61,2% de los 15 millones de usuarios adolescentes de redes sociales en el Perú se encuentran en este entorno de riesgo, urgiendo una reforma integral.

De acuerdo a la tesis presentada por Yupanqui (2025), tesis de la Universidad Privada San Carlos, cuyo objetivo fue determinar los factores que inciden en los delitos ambientales de la zona Ecoturística San José - Huaje, analizando cómo las actividades socioeconómicas descontroladas alteran el medio ambiente en Puno. Aun cuando su investigación adoptó un enfoque cualitativo centrado en un estudio de caso, la metodología correlacional podría proyectarse al explorar cómo la ineficacia regulatoria de Puno se traduce en un incremento del riesgo, no solo físico, sino también digital, donde la falta de fiscalización es la constante. En efecto, el trabajo jurídico revela que la población de San José - Huaje percibe una

contaminación de nivel moderado a grave. Adicionalmente, se constató una correlación positiva considerable que relaciona los factores económicos y sociales con los delitos ambientales. Al fin y al cabo, esta debilidad en el control estatal de Puno, demostrado por la omisión de las instituciones ambientales en su deber de fiscalización, se erige como una amenaza que fomenta la impunidad y que podría ser replicable en la esfera de los delitos informáticos contra la protección de datos.

Prosiguiendo, la tesis presentada por Rosales (2025), tesis de la Facultad de derecho, cuyo objetivo fue determinar la relación entre el aumento de los delitos informáticos y su conexión con la impunidad delictiva, un fenómeno complejo que desborda los controles de investigación debido al carácter anónimo del ciberdelincuente. Seguidamente, la metodología correlacional, de naturaleza cuantitativa y corte transversal, se aplicó con rigurosidad para establecer la intensidad de esta relación en Lima, proporcionando una base empírica indispensable para comprender la creciente vulnerabilidad de la protección de datos. Por un lado, los resultados arrojaron una relación directa positiva alta (Rho = 0,821) entre el incremento de ciberdelitos y la impunidad. Por otro lado, el fraude informático fue identificado como el delito más prevalente con un 71.7%, lo que subraya el peligro constante para el patrimonio y los datos personales. Por consiguiente, el 80% de los encuestados consideró que la complejidad delictiva ha aumentado, sugiriendo que, si la legislación en Lima es considerada poco rigurosa en la persecución de estos actos, la incidencia de vulneraciones de datos personales en Puno podría enfrentar desafíos análogos.

2.1. Bases teóricas

2.1.1. Delitos informáticos

Los delitos informáticos constituyen un tipo de criminalidad que utiliza tecnologías de la información o comunicación como medio, instrumento o escenario de la conducta delictiva, afectando bienes jurídicos como los sistemas informáticos, datos personales, la fe pública, la identidad, el patrimonio y la intimidad. En el Perú, la regulación principal se encuentra en la Ley Nº30096, Ley de Delitos Informáticos, de fecha 21 de octubre de 2013, cuyo Artículo 1 señala que "la presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia" (Yupanqui, 2025).

Por ejemplo, supóngase que una institución local es víctima de un acceso ilícito: un hacker vulnera el sistema informático de la entidad, accede a la base de datos que contiene nombres, direcciones y DNI de ciudadanos, y extrae dicha información para venderla en el mercado negro. En este caso se configura el Artículo 2 de la Ley 30096 ("Acceso ilícito") pues hubo acceso sin autorización y vulneración de medidas de seguridad. El afectado puede presentar denuncia ante la Policía especializada o Fiscalía, solicitar peritaje informático que acredite el "registro de acceso", la "modificación o extracción" del sistema, identificar autor/es, y el Ministerio Público podrá formular acusación. Durante el proceso, la víctima debe salvaguardar logs, respaldos, la custodia de los equipos, y coordinar con el área de TI para la conservación de evidencias. Si el sistema afectado es de una entidad pública o afecta programas sociales, la pena puede agravar según reformas recientes. Otro ejemplo: una persona crea una página web que suplanta la identidad de otra con fines

de estafa, haciéndose pasar por la víctima en medios digitales, lo que constituye el Artículo 9 (Suplantación de identidad) de la Ley 30096. De nuevo, la víctima denunciará, solicitará bloqueo de la web, acreditación de los hechos mediante peritaje, y exigirá reparación. En la práctica, la falta de peritos informáticos o la ausencia de protocolos claros puede demorar la acción y frustrar la tutela.

En cuanto a la efectividad del cuerpo normativo, se ha de reconocer que la tipificación vigente brinda una herramienta para sancionar al autor del delito informático; sin embargo, la viabilidad real muchas veces es limitada por la falta de recursos técnicos y procesales. Por ejemplo, aunque la pena para el Artículo 2 previsiblemente es de 1 a 4 años prisión y 30 a 90 días multa, y para la versión agravada de 3 a 6 años y 80 a 120 días-multa (según modificación), esto no garantiza que muchas denuncias concluyan en condena efectiva. Asimismo, la coordinación interinstitucional (estado-empresa privada) en temas de seguridad informática y Protección de Datos Personales sigue siendo débil, lo que genera zonas de impunidad.

2.1.2. Tipificación legal del delito informático

Si una persona sin autorización accede al sistema informático de una empresa pública vulnerando la clave de administrador y descarga bases de datos personales. Esa conducta se encuadra en el artículo 2 (Acceso ilícito) de la Ley 30096. El fiscal abre investigación, solicita peritaje informático para determinar log de accesos, identifica al autor, y se inicia proceso penal conforme a la tipificación. Otro ejemplo: alguien introduce un malware que borra datos sensibles y hace inaccesible un sistema informático de una entidad privada. Eso configura el artículo 3 (Atentado contra la integridad de datos informáticos). La víctima debe denunciar ante la PNP, aportar evidencias, coordinar bloqueo y preservación de datos, y el Ministerio Público actúa. Sin embargo, si no se dispone de peritos informáticos o los logs no están preservados,

el caso puede quedar impune, lo que evidencia la brecha entre tipificación y operatividad real (Rosales, 2025).

La tipificación legal de los delitos informáticos en el Perú tiene su eje normativo principal en la Ley N.º 30096 ("Ley de Delitos Informáticos"), publicada el 22 de octubre de 2013, la cual establece en su artículo 1 que "la presente Ley tiene por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación, con la finalidad de garantizar la lucha eficaz contra la ciberdelincuencia".

El Capítulo II de dicha ley se denomina "Delitos contra datos y sistemas informáticos" (artículos 2 a 4), luego vienen otros capítulos relativos a delitos contra la indemnidad y libertad sexuales, contra la intimidad, el secreto de las comunicaciones, el patrimonio y la fe pública. Por ejemplo, el artículo 2 tipifica el delito de "Acceso ilícito" (acceder sin autorización a todo o parte de un sistema informático, siempre que se realice con vulneración de medidas de seguridad establecidas). El artículo 3 tipifica el atentado contra la integridad de datos informáticos, el artículo 4 el atentado contra la integridad de sistemas informáticos. Estas tipificaciones configuran la modalidad básica de delito informático.

2.1.3. Hechos descritos que constituyen delitos Informáticos

Los hechos que constituyen delitos informáticos según la Ley N.º 30096 son múltiples y se encuentran descritos de modo pormenorizado en sus artículos. Estos hechos tienen en común su vinculación con sistemas informáticos o datos informáticos, utilizando tecnologías de la información o de la comunicación. La ley organiza los hechos delictivos en varios grupos: delitos contra datos y sistemas informáticos (artículos 2, 3, 4), contra la indemnidad y libertad sexuales (artículos 5, 5-A, etc.),

contra la intimidad y el secreto de las comunicaciones (artículos 7, 8), contra el patrimonio (artículo 8), contra la fe pública, entre otros (Mamanihanco, 2025).

El artículo 3 sanciona el atentado a la integridad de datos informáticos: "El que deliberada e ilegítimamente daña, introduce, borra, deteriora, altera, suprime o hace inaccesibles datos informáticos, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa". El artículo 4 sanciona el atentado contra la integridad de los sistemas informáticos: inutilizar total o parcialmente un sistema informático, impedir acceso, entorpecer funcionamiento, será reprimido con pena privativa de libertad no menor de tres ni mayor de seis años y con ochenta a ciento veinte días-multa.

Si un hacker entra sin autorización al servidor de una empresa municipal, vulnera la clave de administrador, extrae información de ciudadanos y la pública. Ese hecho constituye el artículo 2 (Acceso ilícito). La empresa municipal deberá denunciar ante la PNP, solicitar peritaje, reportar al Ministerio Público, etc. Otro ejemplo: un empleado malintencionado introduce malware que borra miles de registros de clientes de una entidad privada, lo cual constituye el artículo 3 (Atentado a la integridad de datos informáticos). Finalmente, una persona crea una réplica de una página gubernamental para que ciudadanos ingresen datos personales y luego simula la transferencia de esos datos para obtener lucro, lo que constituye el artículo 8 (Fraude informático). En cada caso, la intervención del Estado, la recopilación de evidencia digital, la coordinación interinstitucional, y la capacitación de los actores procesales son factores clave para que la tipificación tenga efecto real.

2.1.4. Existencia de conducta dolosa o culposa tipificada

La tipificación dolosa exige que la investigación establezca que el autor sabía que accedía sin autorización, vulnerando medidas de seguridad. Esto implica peritajes

informáticos que demuestren logs de acceso, vulneración de contraseñas o software malicioso instalado, y que estas acciones fueron emprendidas con conciencia. Si la conducta fuese culposa (por ejemplo, alguien que por descuido dejó una clave sin cambiar y un tercero accede), la norma no contempla explícitamente la culposa para la mayoría de sus tipos: la redacción "deliberada e ilegítimamente" excluye la simple negligencia. Por tanto, la responsabilidad penal conforme a la Ley 30096 se orienta a la conducta dolosa, lo que puede generar un vacío cuando la vulneración se produce por gestión negligente o falta de mantenimiento, pues en tal caso no necesariamente se configura el tipo penal como está redactado (Rojas, 2024).

Un técnico informático de una entidad pública accede sin autorización al servidor y extrae bases de datos de ciudadanos para venderlas: ese acto configura conducta dolosa, pues hubo conocimiento y voluntad de vulnerar el sistema, se aplica el Art. 2 de la Ley 30096 (Acceso ilícito). La fiscalía recoge los logs, entrevista al técnico, acredita que hubo vulneración de medidas de seguridad y se procesa penalmente. En cambio, si un funcionario no actualiza los parches de seguridad y un hacker ingresa por esa falla, podría tratarse de una conducta culposa (negligencia) y no encajar en el tipo doloso: el fiscal podría archivar por falta de voluntad del autor. Esa situación muestra la brecha entre la norma y realidades de gestión institucional.

La víctima o la fiscalía debe denunciar ante la Ministerio Público, o bien ante la Policía Nacional del Perú la conducta sospechosa. La fiscalía abre investigación, solicita peritaje digital para determinar intencionalidad y autorización, preserva cadena de custodia, formula acusación al juez penal si se observa dolo. Si se intentara aplicar el tipo a una conducta culposa (sin voluntad sancionadora), el fiscal podría desestimar por falta de elementos del tipo penal o calificarlo como otro tipo de conducta (responsabilidad civil, administrativa). Esta jerarquía técnica exige capacitación

especializada; sin embargo, en la práctica se encuentran múltiples ineficiencias: falta de peritajes oportunos, escasez de personal especializado, demoras, archivo provisional de denuncias por falta de demostración del dolo.

2.1.5. Correspondencia entre conducta y tipo penal aplicable

El juez o fiscal debe realizar la tipificación adecuada: por ejemplo, si se detecta que el sistema fue inutilizado totalmente, se aplicará el Art. 4 (Atentado contra la integridad de sistemas informáticos) que establece pena de 3 a 6 años prisión y 80 a 120 días multa. Si se presenta suplantación de identidad con perjuicio, corresponde Art. 9 según la modificación por el Decreto Legislativo N.º 1591 de 2023: pena no menor de 3 ni mayor de 5 años, y de 6 a 9 años si la víctima es menor de 18 años y resultó perjuicio (Rojas, 2024).

Asimismo, la correspondencia exige que tanto los operadores como las instituciones comprendan la naturaleza digital del medio y procedimiento: saber que el acceso puede venir de fuera del país, que los datos pueden estar en la nube, que los logs pueden borrarse, que las medidas de seguridad pueden tener fallas, etc. Estas complejidades requieren protocolos especializados, cooperación internacional y actualización normativa. Desde la perspectiva del derecho peruano, el marco es sólido pero su implementación aún es parcial. El reto es hacer que la correspondencia entre conducta y tipo penal no quede en el papel sino se traduzca en sentencias reales.

2.1.6. Modalidad de ejecución del delito

Esta modalidad incluye la utilización de mecanismos tecnológicos, software, hardware, redes de comunicación, dispositivos móviles, programas maliciosos (malware), entre otros, para llevar a cabo una conducta ilícita que vulnera bienes jurídicos como la confidencialidad, la integridad, la disponibilidad de sistemas informáticos, los datos personales, o la fe pública. Según la Ley N.º 30096, el artículo 1 señala que la norma "tiene

por objeto prevenir y sancionar las conductas ilícitas que afectan los sistemas y datos informáticos y otros bienes jurídicos de relevancia penal, cometidas mediante la utilización de tecnologías de la información o de la comunicación" (Portugal, 2024).

Desde la perspectiva del procedimiento penal peruano, cuando se denuncia un delito de modalidad digital, la fiscalía o la Policía Nacional del Perú en su unidad especializada debe identificar la modalidad exacta: ¿se accedió sin autorización? ¿Se alteraron datos? ¿Se interceptó una transmisión? ¿Se utilizó suplantación de identidad o fraude tecnológico? En dicha identificación radica la correcta tipificación y la efectiva persecución penal.

No obstante, existen deficiencias que afectan la operatividad de estas modalidades: la rápida evolución de la tecnología hace que muchas modalidades emergentes no estén completamente previstas o adaptadas en la normativa; la falta de capacitación técnica en peritos informáticos y la ausencia de protocolos estándar de investigación difuminan la correcta determinación de la modalidad; la prueba digital es volátil (logs borrados, dispositivos cambiados, nube) y exige acciones inmediatas que no siempre se realizan. Esta realidad reduce la eficacia del cuerpo normativo y la posibilidad de sanción.

2.1.7. Uso de medios tecnológicos para vulnerar sistemas o redes informáticas

Si un grupo de ciberdelincuentes lanza un ataque DDoS contra el portal web de una empresa de servicios públicos, usando una red de bots automatizados para colapsar el sistema y exigir rescate (ransomware funcional). Allí el medio tecnológico es la red de bots, el exploit, el software de cifrado. La empresa presenta denuncia ante la PNP-unidad de ciberdelincuencia; se realiza peritaje que identifica direcciones IP remotas, se asegura la evidencia, se coordina con fiscalía para acusar bajo el artículo 4 (Atentado contra la integridad de sistemas informáticos). Otro ejemplo: un phishing masivo que instala troyano para robar credenciales bancarias. El medio tecnológico (correo falso, troyano) constituye

la base del delito; sin estos medios, la conducta no podría concretarse. Si la investigación no logra identificar el mecanismo (por ejemplo, si el malware fue eliminado), la sanción puede fracasar (Quincho et al., 2025).

Si la identificación del medio tecnológico exige peritajes forenses digitales, análisis de logs, recuperación de evidencias, y cooperación entre entidades técnicas y fiscales. El proceso comienza con denuncia, aseguramiento de evidencias, apertura de investigación fiscal, solicitud de medidas cautelares, peritaje digital y acusación. Sin embargo, las deficiencias son marcadas: la capacidad técnica estatal es limitada, muchas entidades no cuentan con "sandbox" para análisis de malware, y las demoras afectan la trazabilidad de los medios usados. Además, la ley se ve retada por nuevas tipologías: el uso de criptomonedas para monetizar datos robados, los servicios de cibercrimen "as a service", los ataques automatizados, etc. Como lo advierte un análisis sobre la implementación de la Ley N.º 30096, "existe un desfase entre la tipificación y la operatividad práctica" debido a estos retos técnicos.

2.1.8. Utilización de mecanismos de suplantación o fraude digital

Para que esta modalidad configure delito es preciso que exista:

- Creación o uso de instrumentos de suplantación (sitio web falso, interfaz clonada, correo fraudulento)
- Engaño de la víctima o manipulación de su credibilidad
- Obtención de un provecho ilícito o perjuicio al tercero
- Utilización de medio informático.

En el procedimiento, la fiscalía debe acreditar el modus operandi (phishing, clonación, explotación de vulnerabilidad), la existencia del perjuicio (económico, patrimonial, moral) y la vinculación entre suplantación/fraude y medios digitales (Echeverría & Salvador, 2024).

Por ejemplo, un sujeto crea un sitio web que imita el portal de una entidad gubernamental para que los ciudadanos ingresen sus datos personales de banca electrónica, los cuales luego usa para transferencias ilegales. Este mecanismo de suplantación/fraude corresponde al artículo 8 (Fraude informático) y/o al artículo 9 (Suplantación de identidad) de la Ley 30096. La víctima denuncia, se recaba evidencia digital (registro del sitio falso, transferencias, logs de host), la fiscalía formula acusación. Si no se preservó la evidencia o se borraron los logs, la acción penal puede quedar frustrada. Otro ejemplo: un trabajador malicioso dentro de una empresa clona la interfaz del sistema interno y solicitó datos a otros empleados que respondieron, pensando que era legítima la página; acto que constituye fraude informático. En la práctica, sin protocolos internos de seguridad y sin sensibilización del personal, esta modalidad prospera.

Además, la normativa, aunque contempla el fraude y la suplantación, requiere mayor actualización para abarcar nuevas formas (deepfake, inteligencia artificial). Investigaciones recientes destacan que "la ineficacia de la Ley 30096 en el delito de suplantación de identidad por medios informáticos" guarda relación con la ausencia de especificación técnica de ciertas modalidades.

2.1.9. Acceso, interceptación o alteración no autorizada de datos personales

La Ley N.º 29733 (Ley de Protección de Datos Personales) establece el derecho fundamental del titular a la autodeterminación informativa (art. 2 inc. 6 de la Constitución Política del Perú) y dispone en su reglamento la obligación de adoptar medidas de seguridad para la protección de datos personales. Desde la perspectiva penal, esta modalidad exige que se acredite:

- Acceso, interceptación o alteración de datos personales sin autorización
- Que dichos datos formen parte de un sistema informático o de comunicaciones

- Que exista vulneración de medidas de seguridad, o que se haya excedido lo autorizado
- Que haya perjuicio real o potencial al titular de los datos o a terceros (Intriago & Chancay, 2024).

Un servidor público guarda datos personales de ciudadanos en una base de datos sin cifrar; un ciberdelincuente vulnera la medida de seguridad, accede y extrae los datos, difundiéndolos en foros públicos. Esto configura "acceso ilícito" (art. 2 Ley 30096) y "atentado a la integridad de datos informáticos" (art. 3 Ley 30096) y viola el derecho a protección de datos personales garantizado por la Ley 29733. La víctima denuncia, se realiza peritaje, se identifican logs y dirección IP, se coordina entre la entidad pública, Policía y fiscalía para sancionar al autor. Otro ejemplo: una entidad privada sufre filtración de una base de datos de clientes que contiene números de DNI, correos, datos biométricos; investigación revela que falta control de acceso, no hubo cifrado y los datos fueron vendidos. Aquí la alteración/no autorización y la falta de medida de seguridad llevan a responsabilidad tanto penal como administrativa.

2.1.10. Responsabilidad y efectos jurídicos

En el ámbito de los delitos informáticos, la responsabilidad se configura cuando se comete una conducta típica, antijurídica, culpable (en general con dolo, ya que la mayoría de los tipos de la Ley N.º 30096, Ley de Delitos Informáticos exigen "deliberada e ilegítimamente" como inicio del tipo) (Calderón, 2024).

La responsabilidad puede recaer sobre la persona natural que comete la conducta, pero también existen implicaciones civiles y administrativas: la víctima puede exigir reparación del daño, el Estado puede iniciar acciones de responsabilidades por negligencia institucional, y la entidad privada puede ser objeto de sanciones de carácter civil o administrativo por falta de medidas de seguridad

adecuadas. En términos penales, la Ley 30096 calcula penas privativas de libertad y días-multa para los delitos tipificados (por ejemplo, el Artículo 2, acceso ilícito: pena no menor de 1 ni mayor de 4 años y 30 a 90 días-multa), y tras la reforma (Decreto Legislativo N.º 1614 del 21 de diciembre de 2023) se endurecieron ciertas sanciones.

2.1.11. Identificación de sujetos activos y pasivos involucrados en delitos informáticos

Supóngase que un programador de una empresa privada modifica el sistema informático de su empleador para extraer datos personales y venderlos a terceros. En ese caso, el sujeto activo es el programador (intraneus), el sujeto pasivo la empresa y los titulares de los datos personales. La fiscalía investigadora puede ordenar allanamiento en la oficina, peritaje de la máquina, preservación de correos, formular acusación. En otro caso, un atacante externo desde otro país vulnera el servidor de un banco peruano. Allí el sujeto activo es externo, el banco es sujeto pasivo institucional, los clientes del banco son también sujetos pasivos (Hinojo et al., 2022).

La identificación de sujetos activos y pasivos tiene consecuencias procesales y de política criminal: permite definir la competencia funcional (fiscalía especializada, unidad de ciberdelincuencia), establece qué medidas deben adoptarse (allanamiento, intervención de comunicaciones, geolocalización), y permite que los encargados del sistema (responsables de TI) reconozcan su obligación de resguardar la infraestructura.

No obstante, existen graves retos: muchos delitos informáticos implican autores que operan desde el extranjero, con dispositivos ubicados fuera de la jurisdicción peruana, lo que dificulta la individualización del sujeto activo. Como advierte una investigación, "la no individualización del ciberdelincuente" es uno de los factores que contribuyen a la impunidad.

2.1.12. Existencia de daño digital, patrimonial o reputacional derivado del hecho delictivo

En el procedimiento penal, la fiscalía debe identificar, calcular o estimar el

monto patrimonial afectado, documentar el perjuicio (transferencias no autorizadas, pérdida de negocios, gastos de mitigación) o evidenciar la reputación dañada (pérdida de clientes, divulgación pública de datos personales). En la práctica peruana, el desafío es que muchos daños digitales no se denuncian o no se cuantifican adecuadamente: la víctima no sabe que sufrió la vulneración (por ejemplo, filtración de datos personales) o no dispone de los medios para acreditarlo; además, los sistemas vulnerados a menudo no tienen respaldo o logs, lo que impide estimar el alcance del daño. Según informe de la Defensoría del Pueblo del Perú, la impunidad en delitos informáticos está vinculada a la falta de evidencia técnica y a la banalización del riesgo digital (Benavides & Mercedes, 2021).

La responsabilidad de la entidad que sufría el ataque puede también entrar en juego si la falta de medidas de seguridad contribuyó al daño, lo que abre vías administrativas (Ley 29733) además de penales. De esta forma, la realidad demuestra que la tipificación es solo el punto de partida, la gestión del daño y la reparación efectiva requieren estructura institucional y técnica robusta.

2.1.13. Existencia de denuncia o proceso penal en curso vinculado a cibercrimen

La denuncia debe ser acompañada de información mínima: descripción del hecho, medios tecnológicos afectados, posible autor, indicios de prueba (logs, correos, accesos). Luego la fiscalía procede con la investigación preliminar, puede solicitar medidas de urgencia (allanamientos, interceptación de datos, geolocalización). Si la fiscalía considera que existen méritos, formula acusación y el juez inicia el proceso penal. En muchos casos, sin embargo, la fase preliminar se extiende sin resultado, lo que genera dilación y desincentivo a las víctimas. La investigación penal peruana en ciberdelincuencia requiere tiempos reducidos, pero la velocidad del mundo digital demanda intervención inmediata (Paccori, 2021).

Cabe mencionar que la fiscalía cuenta con la Unidad Fiscal Especializada en Ciberdelincuencia (UFEC) con presencia en 34 distritos fiscales como apoyo técnico para delitos informáticos. Una vez recibida la denuncia, se activan diligencias de preservación de evidencia digital, solicitudes de medidas cautelares y el peritaje informático que sustentará la acusación.

2.1.14. Derecho a la protección de datos personales

Este reconocimiento constitucional da lugar a que el tratamiento de datos personales, es decir, la recolección, registro, almacenamiento, utilización, transferencia, supresión o cualquier otra operación con datos que identifiquen o hagan identificable a una persona, sea regulado bajo un marco normativo específico. En el Perú, el instrumento legal clave es la Ley N.º 29733, Ley de Protección de Datos Personales, aprobada el 3 de julio de 2011, cuya finalidad es "garantizar el derecho fundamental a la protección de los datos personales" mediante un tratamiento adecuado de los mismos (Paccori, 2021).

Una municipalidad vulnerable filtra datos personales de ciudadanos (nombres, DNI, correos) por falta de seguridad. Los titulares pueden exigir a la entidad que informe quién accedió a la base de datos, cómo, con qué finalidad, y pueden requerir supresión o corrección de los datos. Si esto no ocurre, pueden acudir a la ANPD para interponer queja o incluso optar por demanda.

2.1.15. Principio de consentimiento y autodeterminación informativa

El principio de consentimiento exige que el tratamiento de datos personales solo se realice cuando medie consentimiento libre, previo, expreso e inequívoco del titular, salvo que la ley disponga otra base legal de tratamiento. Así lo señala la Ley 29733 en su artículo 3 (datos personales) en concordancia con el artículo 13.5 del mismo cuerpo normativo: "Los datos personales solo pueden ser objeto de

tratamiento con consentimiento del titular, salvo que la ley autorice otro tipo de tratamiento" (Huaman y Pita, 2024).

2.1.16. Existencia de consentimiento previo, libre y expreso del titular (Ley N.º 29733, art. 12)

El artículo 12 del Reglamento de la Ley 29733 y normas complementarias establecen que el consentimiento debe cumplir los requisitos de ser previo, libre, expreso e inequívoco cuando se realice el tratamiento de datos personales. Si no se acredita este consentimiento, el tratamiento puede ser ilícito y el titular puede reclamar nulidad del tratamiento, supresión de datos, indemnización por daños y perjuicios. La ANPD, en sus directivas, exige que se documente el consentimiento en bases de datos que contengan datos sensibles o transferencia internacional (De León y Salgado, 2022).

En la práctica peruana, algunas entidades no documentan adecuadamente el consentimiento o utilizan cláusulas generales poco informadas, lo que debilita la protección del titular. Además, cuando el consentimiento es masivo o automático (por ejemplo "acepto términos y condiciones" sin claridad) se cuestiona su libertad e información. Esto vulnera la autodeterminación informativa y reduce la efectividad del sistema. Se requiere cultura organizacional, auditoría, y supervisión de la ANPD para asegurar que el consentimiento cumpla con los requisitos.

Si una empresa de marketing pretende recopilar datos de clientes para enviar ofertas. Envía un formulario que dice "acepto recibir comunicaciones" sin explicar el uso de los datos, la duración, ni si transferirá a terceros. Dicho consentimiento no es libre ni informado. En cambio, si el formulario contiene explicaciones claras, finalidades específicas, se otorga con firma electrónica y se permite revocar, entonces cumple los requisitos. Si la empresa actúa sin ese consentimiento, el cliente puede exigir supresión de los datos, presentar queja ante la ANPD, y la empresa

podría ser sancionada.

2.1.17. Registro documental del consentimiento otorgado

El registro documental del consentimiento otorgado es un requisito indispensable para que el tratamiento de datos personales sea lícito en el marco del sistema peruano. Bajo la Reglamento de la Ley N.º 29733 (Decreto Supremo 003-2013-JUS) y normas complementarias, el responsable o encargado del banco de datos debe conservar la evidencia del consentimiento otorgado por el titular, ya sea mediante firma manuscrita, digital, electrónica o por otros medios que aseguren la integridad, autenticidad y trazabilidad de la manifestación de voluntad (Raymundo, 2025).

En el Perú se identifican debilidades: muchas instituciones no implementan sistemas de registro digital, los formularios son genéricos y no contienen información concreta, los consentimientos se dan en masa sin verificación individual, o los registros no se conservan de forma organizada. En consecuencia, cuando ocurre una vulneración de datos personales y se inicia investigación administrativa o judicial, la entidad no puede presentar pruebas del consentimiento, lo que dificulta la defensa y la aplicación de sanciones. Esta brecha debilita la eficacia del régimen de protección de datos y reduce la confianza de los titulares.

2.1.18. Información clara sobre fines, uso y tratamiento de los datos personales

Conforme al artículo 4 de la Ley N.º 29733 – Ley de Protección de Datos Personales, uno de los principios rectores es el de finalidad: los datos personales solo pueden recolectarse para fines determinados, explícitos, legítimos y comunicados al titular, y no pueden tratarse posteriormente de una forma incompatible con dichos fines. Además, el Reglamento de la ley (el Decreto Supremo N.º 003-2013-JUS aprobó el 22 de marzo de 2013) implica la obligación de que el responsable del banco de datos informe al titular, antes de recoger los datos, acerca de: la identidad del responsable, la

finalidad del tratamiento, la forma de ejercer los derechos del titular, la posibilidad de revocar el consentimiento, entre otros (Torres, 2025).

Sin una información previa clara, el consentimiento pierde legitimidad, lo cual podría derivar en la nulidad del tratamiento. Segundo, reduce la asimetría de información entre la entidad responsable y el titular, fortaleciendo la autodeterminación informativa. Tercero, posibilita que los titulares ejerzan sus derechos ARCO (Acceso, Rectificación, Cancelación, Oposición) con conocimiento concreto del uso que se hará de sus datos.

En la práctica peruana, la exigencia de información clara enfrenta varios retos: muchas entidades diseñan formularios genéricos ("Acepto los términos y condiciones") sin detallar finalidades específicas, duración del tratamiento, transferencia a terceros o uso para marketing. Además, los textos suelen estar en letra pequeña, con lenguaje técnico-jurídico, lo que impide el real entendimiento por parte del titular. Estas deficiencias debilitan la operatividad del principio de transparencia. Si se produce una vulneración de datos y el responsable no demostró que proporcionó información clara, la sanción administrativa por parte de la Autoridad Nacional de Protección de Datos Personales (ANPD) puede tener mayor fundamento, ya que dicho incumplimiento constituye una infracción. Estudios y manuales de la Defensoría del Pueblo advierten que, sin una cultura de información clara y veraz, el derecho a la protección de datos personales queda en riesgo.

2.1.19. Principio de seguridad y confidencialidad

En el artículo 10 de la Ley 29733 se dispone que el responsable del banco de datos debe adoptar las "medidas de seguridad que permitan mantener la confidencialidad, integridad y disponibilidad de los datos personales". El Reglamento, en sus artículos 28 a 32 (o su equivalente actualizado en el nuevo

reglamento de 2024) detalla que las medidas deben ser "aptas, eficaces, acorde con la categoría de datos personales y el riesgo que su tratamiento implica" (Muñoz, 2025).

En el caso de vulneración, debe existir un proceso de gestión de incidentes que incluya notificación al titular y a la ANPD. Una vulneración del principio puede generar responsabilidad administrativa para la entidad, e incluso responsabilidad penal si el caso trasciende al ámbito de los delitos informáticos. En la práctica peruana se encuentran deficiencias significativas: auditorías descubren que bases de datos de entidades vulnerables carecen de cifrado, que no se registran accesos, que los sistemas de respaldo no están en ambientes seguros o que los logs se sobrescriben sin control. Estos déficits ponen en riesgo la confidencialidad y disponibilidad de los datos personales. Por ejemplo, la filtración de bases de datos estadales o municipales ha sido recurrente, lo que evidencia que el principio, aunque normativamente exigido, no siempre se materializa.

2.1.20. Existencia de medidas técnicas y organizativas para la protección de datos personales (Reglamento, arts. 28–32)

El vínculo entre el principio de seguridad y confidencialidad y la existencia concreta de medidas técnicas y organizativas es directo y obligatorio. En el Reglamento aprobado por el Decreto Supremo 003-2013-JUS, los artículos 28 al 32 señalan que los responsables de bancas de datos deben implementar, de forma documentada, medidas de seguridad tales como: evaluación de riesgos, políticas de tratamiento, clasificación de datos personales, control de acceso y auditorías, cifrado, backup, recuperación ante desastres, así como capacitación del personal (Calderón et al., 2024).

Desde el punto de vista funcional, las medidas técnicas se refieren a aspectos

informáticos (firewalls, antivirus, cifrado, control de accesos, sistemas de detección de intrusos), mientras que las medidas organizativas abarcan políticas de seguridad, protocolos de acceso, registro de incidentes, asignación de responsabilidades, evaluación de impacto, contratos con encargados de tratamiento, monitoreo y auditoría constantes. El nuevo reglamento de 2024 (Decreto Supremo N.º 016-2024-JUS) refuerza estos requisitos actualizándolos a estándares internacionales como ISO/IEC 27001, imponiendo la figura del Oficial de Datos Personales, evaluación de impacto y reporte de incidentes en plazos concretos.

En el caso que una entidad pública diseña un plan de protección de datos que incluye: política de seguridad aprobada por la gerencia, clasificación de datos sensibles, cifrado de bases, acceso por doble autenticación, respaldo diario en nube con encriptado, auditoría semestral, registro de incidentes y oficial de datos designado. Luego sufre un intento de intrusión que es detectado por el sistema IDS, se activa protocolo de respuesta, se bloquea el acceso, se notifica al titular y a la ANPD en 48 horas. Este escenario cumple con las medidas técnicas y organizativas. Por el contrario, un municipio que solo guarda los datos en un servidor local sin cifrado, sin backups, sin registro de accesos ni política de seguridad, y que nunca ha auditado, se encuentra en incumplimiento. Una vulneración ahí compromete no solo los datos sino la responsabilidad de la entidad ante la ANPD y los titulares.

2.1.21. Existencia de protocolos de acceso, resguardo y manejo de información confidencial

Estos protocolos deben cubrir: quién tiene acceso a qué datos, registro de accesos, control de privilegios, autorización de usuarios, verificación de identidades, procedimientos de respaldo, plan de contingencia, tratamiento de incidentes, y la restricción del acceso a datos sensibles (Pandia, 2024).

La existencia de estos protocolos es relevante porque permite demostrar que

la entidad ha cumplido con su obligación de seguridad. En caso de vulneración, si no se puede demostrar que existían y se aplicaban protocolos adecuados, la entidad se enfrenta a sanciones administrativas e incluso puede tener responsabilidad civil por daños causados a titulares de datos. Por ejemplo, el artículo 33 del nuevo reglamento de 2024 expedido como Decreto Supremo 016-2024-JUS prevé la obligación de reportar incidentes de seguridad en un plazo máximo de 48 horas a la ANPD. (Nota: verificación conforme al reglamento).

Entonces si una universidad privada cuenta con protocolos formales: solo personal autorizado de TI tiene acceso al servidor; los datos sensibles están en carpetas con permisos especiales; cada acceso es registrado con usuario y hora; se realizan copias de seguridad cada noche a servidor externo; se realiza simulacro de intrusión cada seis meses; existe plan de respuesta que incluye notificación a la dirección y al titular en caso de incidente. Gracias a ello, un intento de acceso no autorizado fue bloqueado, se aisló el servidor comprometido, se notificó al titular y se activó la ANPD. En cambio, una municipalidad que no tiene protocolos formales tuvo que enfrentar la filtración de datos de beneficiarios de programas sociales porque su servidor tenía acceso compartido, contraseñas por defecto, sin registro de accesos ni respaldo externo. Esa situación resultó en sanción de la ANPD y reclamos de los titulares.

2.1.22. Realización de auditorías o controles internos en materia de ciberseguridad

La realización de auditorías o controles internos en materia de ciberseguridad constituye una pieza estratégica dentro del régimen de protección de datos personales y de sistemas informáticos. En el contexto peruano, este requisito emerge tanto del marco normativo de protección de datos, Ley N.º 29733 ("Ley de Protección de Datos Personales"), como del régimen de los delitos informáticos, Ley N.º 30096

("Ley de Delitos Informáticos"), y de su reglamentación asociada. Según el artículo 16 de la Ley 29733, el titular del banco de datos personales debe adoptar "medidas técnicas, organizativas y legales que garanticen su seguridad y eviten su alteración, pérdida, tratamiento o acceso no autorizado" (Barroso et al., 2023).

No obstante, en la práctica peruana existen desafíos reales: muchas entidades, especialmente municipalidades o instituciones con poco presupuesto, no han implementado auditorías regulares; la falta de peritos en ciberseguridad, la escasa integración del área legal, tecnología e informática, así como la cultura de prevención poco desarrollada, hacen que los controles internos sean ineficaces o meramente formales. Un reporte reciente indica que la ANPD impuso sanciones mayores a S/ 7.6 millones en 2023 tras detectar incumplimientos de medidas de seguridad.

2.1.23. Vulneración y consecuencias jurídicas

Tal vulneración tiene consecuencias jurídicas en diversas dimensiones: penal, administrativa y civil. En el plano penal, cuando la conducta encaja en uno de los tipos de la Ley 30096 (por ejemplo, acceso ilícito, atentado contra datos, fraude informático), la víctima o el Estado pueden promover investigación fiscal y enjuiciamiento. En el plano administrativo, la Ley 29733 y su reglamento establecen infracciones sancionables por la ANPD, con multas que pueden ir desde 0,5 hasta 100 UIT (Unidad Impositiva Tributaria) (Ramos, 2024).

Las consecuencias jurídicas son variadas:

- Para la entidad responsable o el encargado del tratamiento, puede imponerse sanción administrativa, multa o medida correctiva
- Para el autor de la vulneración se puede iniciar proceso penal si se trata de delito informático
- Para el titular afectado se abre la vía de reparación civil

- Reputacional mente, la entidad puede perder la confianza de sus usuarios, lo que repercute en su viabilidad y continuidad operativa.

2.1.24. Exposición, filtración o comercialización no autorizada de datos personales

La Ley 29733 y su reglamento regulan el tratamiento, obligación de seguridad y sanción de infracciones: el artículo 133 del nuevo reglamento clasifica como infracción grave "no inscribir o actualizar los bancos de datos personales", y como infracción muy grave "no realizar el tratamiento de datos sensibles con las medidas de seguridad pertinentes".

La responsabilidad normativa también se extiende a la confidencialidad, integridad y disponibilidad del dato; cuando los datos se comercializan, el daño potencial al titular es elevado: robo de identidad, fraude, reputación afectada, pérdida de empleo, etc. Jurídicamente, la exposición o comercialización puede derivar en responsabilidad penal del autor (si se configura delito informático), administrativa de la entidad (sanción de la ANPD), y civil por reparación del daño (Mamanihanco, 2025).

2.1.25. Afectación a la privacidad, honra o identidad digital del titular

El daño a la privacidad, honra o identidad digital del titular de datos personales es una de las consecuencias más graves e insidiosas de las vulneraciones informáticas y de datos en el contexto peruano. Desde el punto de vista normativo, el derecho a la protección de los datos personales está consagrado en el art. 2, numeral 6 de la Constitución Política del Perú, que establece el derecho de toda persona a que los servicios informáticos, computarizados o no, no suministren informaciones que afecten su intimidad personal o familiar (Mamanihanco, 2025a).

La honra implica el buen nombre, la reputación, la consideración que tiene una persona en sociedad; la identidad digital refiere al conjunto de datos y rastros de una

persona en el entorno digital que permiten identificarla, rastrearla o suplantarla. En el contexto peruano, este último concepto ha cobrado relevancia a partir de la digitalización de trámites, la plataforma ID GOB PE para identidad digital (Marco de identidad digital del Estado Peruano) y los crecientes riesgos de suplantación.

Cuando se vulnera la privacidad o identidad digital, se abren varias posibles vías de tutela:

- Vía penal, si la conducta encaja en uno de los tipos de la Ley N.º 30096 – Ley de Delitos Informáticos (por ejemplo, suplantación de identidad digital, fraude informático, etc.)
- Vía administrativa-sancionadora por la ANPD (Autoridad Nacional de Protección de Datos Personales) si la entidad responsable incumplió la Ley 29733 o su Reglamento;
- Vía civil, mediante demanda de indemnización por daños morales o patrimoniales.

Por ejemplo, si se filtran datos de salud de un titular y aparecen en Internet, se lesiona su intimidad, su honra y su identidad digital; la entidad que almacena los datos puede responder administrativamente, los responsables pueden tener responsabilidad penal, y la persona afectada puede exigir reparación.

2.1.26. Registro de denuncias ante la Autoridad Nacional de Protección de Datos Personales o el Ministerio Público

Una persona descubre que una empresa privada usó sus correos sin consentimiento para fines comerciales. Ingresa a la web de la ANPD, completa el formulario de denuncia (adjunta capturas, contrato de servicio, correo recibido) y recibe un código de seguimiento. La ANPD abre expediente, solicita a la empresa información, y sanciona con multa de 10 UIT. En paralelo, se informa al Ministerio

Público para evaluar si hay aspecto delictivo (uso indebido de datos personales). Si el usuario hubiese ignorado denunciar, la conducta habría permanecido impune y la empresa podría seguir el tratamiento sin sanción (Marabel, 2021).

Desde el punto de vista jurídico-procesal, registrar la denuncia implica varias etapas:

- Presentación de la denuncia (online o presencial) que detalle el hecho, datos del responsable o entidad, posibles pruebas (logs, capturas, correos, contratos)
- La ANPD evalúa competencia y atribuye el expediente, solicita información al responsable del banco de datos, puede imponer medidas provisionalísimas;
- Si hay indicios de delito informático, la fiscalía puede asumir competencia, solicitar peritaje informático, medidas cautelares, y formular acusación. La Ley 29733 y su Reglamento regulan los plazos, procedimiento y sanciones administrativas; el nuevo Reglamento por Decreto Supremo N.º 016-2024-JUS refuerza la obligación de reporte de incidentes en 48 h y el régimen de fiscalización.

2.3. Marco conceptual

Delito informático

Se entiende como aquella conducta típica, antijurídica y culpable que utiliza tecnologías de la información o de la comunicación como medio, instrumento o escenario para afectar sistemas informáticos, datos personales o bienes jurídicos vinculados (Rivas, 2024).

Vulneración

Se entiende al quebrantamiento, violación o afectación del derecho a la protección de los datos personales. En este marco, se considera cómo los actos informáticos pueden generar dicha vulneración: la pérdida de confidencialidad, la

alteración sin autorización, el acceso indebido o la cesión no consentida de datos personales. (Aredo, 2021)

Derecho a la protección de datos personales

Este derecho comprende el reconocimiento de que toda persona tiene la facultad de controlar su información personal y que ésta debe ser tratada con respeto a su intimidad y otros derechos fundamentales. En el contexto latinoamericano y peruano, se observa que la normativa y la práctica permiten vulneraciones que exigen un marco conceptual preciso. (Rivas, 2024).

Informáticos

En el presente estudio, se refiere a los sistemas, herramientas y medios tecnológicos mediante los cuales se ejecutan actos o conductas que afectan la seguridad, integridad o confidencialidad de los datos personales. (Rivas, 2024).

CAPITULO III

METODOLOGÍA DE INVESTIGACIÓN

3.1. Enfoque de investigación

El presente estudio se orienta bajo el enfoque cuantitativo, el cual, según García (2021), persigue cuantificar y analizar fenómenos mediante datos numéricos, empleando un método riguroso y sistemático para obtener conclusiones válidas y generalizables. En el marco de esta investigación descriptivo-correlacional, el enfoque cuantitativo permitió medir variables como la frecuencia percibida de los delitos informáticos, la vulneración del derecho a la protección de datos personales, y la percepción de la adecuación de la normativa y las capacidades institucionales, mediante un instrumento estructurado y precodificado.

3.2. Método de la investigación

Este enfoque parte de principios generales acerca de la relación entre delitos informáticos y vulneración del derecho a la protección de datos personales, formula predicciones específicas (hipótesis) y posteriormente las verifica mediante la encuesta aplicada a la ciudad de Puno. Según diversas fuentes, el método hipotético – deductivo "consiste en desarrollar aplicaciones o consecuencias concretas a partir de principios generales" y se caracteriza porque la conclusión se deriva lógicamente de las premisas planteadas. (Gómez, 2022)

3.3. Tipo de investigación

Según Gómez (2022), el estudio básico busca profundizar en la comprensión de principios o leyes científicas, más que en su aplicación inmediata a casos prácticos o soluciones directas. En este sentido, el estudio descriptivo-correlacional permite observar y medir variables tal como se presentan en su contexto natural (la ciudad de Puno), y establecer las relaciones entre ellas, por ejemplo, entre la percepción del aumento de la ciberdelincuencia y la evaluación de la adecuación normativa, sin introducir cambios en el entorno o el comportamiento de los participantes.

3.4. Nivel de investigación

Se empleó el nivel explicativo, que de acuerdo con Rus (2021), se enfoca en la tarea de esclarecer y comprender las relaciones de causa y efecto entre dos variables de estudio. Además, esta metodología ayuda a comprender las razones subyacentes que explican los casos o desafíos, considerando no solo el motivo de su origen, sino también la forma en que se llevan a cabo.

3.5. Diseño de investigación

Se hizo uso del diseño no experimental – transversal; el mismo que se enfoca en el estudio y observación de la problemática y desafíos sin intervenir deliberadamente en los elementos identificados para a posterior se lleve un análisis en un tiempo determinado, teniendo en cuenta la consideración de su importancia en el contexto transversal (Huaire, 2019).

3.6. Ámbito de investigación

La investigación se desarrolló en la ciudad de Puno, Perú, durante los años 2021-2022, con el propósito de analizar la incidencia de los delitos informáticos en la vulneración del derecho a la protección de datos personales, así como la adecuación normativa e institucional para su prevención y sanción. Este ámbito

geográfico y temporal permite comprender las percepciones y realidades de las instituciones locales (públicas y privadas) y de los operadores del sistema de justicia en un contexto específico, caracterizado por avances tecnológicos, brechas institucionales y retos normativos.

3.7. Población y muestra.

3.7.1. Población

La población objeto del presente estudio estuvo constituida por 84 profesionales, organizados de la siguiente manera:

38 especialistas adscritos a la División de Investigación de Delitos de Alta Tecnología (DIVINDAT) de la Policía Nacional del Perú, cuya labor comprende la identificación, rastreo, análisis forense digital y acreditación de evidencias relacionadas con ilícitos informáticos cometidos mediante redes y sistemas telemáticos.

46 abogados con especialización en derecho informático, ejercientes en la ciudad de Puno, cuya práctica profesional se orienta a la asesoría, litigación y defensa de los derechos asociados a la privacidad, protección de datos personales, identidad digital y responsabilidad penal tecnológica.

La combinación de ambos grupos permite un abordaje integral del fenómeno investigado, articulando el plano técnico-operativo relativo al esclarecimiento de conductas ilícitas con el plano jurídico-normativo, vinculado al resguardo del derecho fundamental a la protección de datos personales, reconocido por el artículo 2 inciso 6 de la Constitución Política del Perú y desarrollado por la Ley N°29733.

3.7.2. Muestra

La muestra corresponde a un subconjunto estadísticamente pertinente de la población descrita. Se seleccionaron sujetos que representan, de manera

proporcional, la experiencia tanto en investigación penal de ciber incidentes, como en defensa y tutela jurídica de datos personales frente a vulneraciones derivadas de delitos informáticos.

Se aplicó un muestreo probabilístico, conforme a lo expuesto por Vara (2015), asegurando que cada integrante de la población tenga la misma probabilidad de formar parte de la muestra. La determinación del tamaño muestral se efectuó mediante la fórmula para poblaciones finitas:

$$n = \frac{Z^2 \cdot p \cdot (1 - p)}{e^2}$$

Donde:

- n = tamaño de la muestra
- Z = valor crítico según nivel de confianza (1.96 para 95%)
- p = proporción estimada (0.5 como criterio conservador)
- e = margen de error permitido (0.05)

Como resultado del procedimiento estadístico, se obtuvo una muestra de 69 profesionales, número considerado adecuado para reflejar criterios especializados respecto a la incidencia de los delitos informáticos en la vulneración del derecho a la protección de datos personales dentro del contexto territorial y temporal de estudio.

3.8. Técnicas e instrumentos para la recolección de información

3.8.1. Técnica de la investigación

En esta investigación descriptivo-correlacional se empleó la técnica de la encuesta como mecanismo principal de recolección de información. Conforme a lo planteado por Juana Casas Anguita y colaboradores (2003), la encuesta constituye un procedimiento estandarizado de investigación mediante el cual se recogen datos

de una muestra representativa de una población, con el fin de explorar, describir y correlacionar variables específicas.

3.8.2. Instrumentos

En la presente investigación se utilizó un cuestionario precodificado como instrumento de recolección de datos, el cual permite obtener cuantitativamente información estructurada y estandarizada de los participantes. Según la metodología académica de Juana Casas Anguita et al. (2003), la encuesta con cuestionario precodificado representa una herramienta fundamental para recoger respuestas fiables y susceptibles de análisis estadístico, ya que cada alternativa de respuesta se asigna previamente un código numérico.

3.9. Recogida de Datos

3.9.1 Validación

Para garantizar la validez del instrumento de recolección de datos se aplicó el método de juicio de expertos, en el que profesionales especializados en el tema de los delitos informáticos, protección de datos personales y métodos cuantitativos revisaron cuidadosamente el cuestionario. Estos expertos evaluaron que los ítems fuesen pertinentes al constructo que se pretende medir (es decir, la incidencia de los delitos informáticos en la vulneración del derecho a la protección de datos personales), que su redacción fuera adecuada en contenido y forma, que se ajustaran al contexto peruano y al marco normativo (como la Ley Nº30096 y la Ley Nº29733), y que fueran comprensibles para la población objeto del estudio en la ciudad de Puno.

3.9.2. Confiabilidad

Para verificar la fiabilidad del instrumento utilizado en este estudio descriptivo correlacional, se llevó a cabo una prueba psico-estadística que permitió asegurar la consistencia interna y la precisión de las mediciones. Este proceso implicó aplicar el

cuestionario precodificado a un grupo piloto y calcular el coeficiente de fiabilidad (por ejemplo, el Alfa de Cronbach) para cada uno de los bloques temáticos (por ejemplo: modalidad de delitos informáticos, medidas de seguridad institucional, percepción de vulneración de datos). De este modo, se pudo constatar la estabilidad del instrumento en condiciones repetidas, es decir, que bajo contextos similares los resultados serían homogéneos, lo que garantiza que las mediciones obtenidas reflejen con fiabilidad el fenómeno estudiado. Estudios metodológicos señalan que la confiabilidad es un requisito indispensable para que los datos estén libres de errores sistemáticos y fortalezcan la validez de los resultados, permitiendo un análisis correlacional más robusto y riguroso del problema de investigación.

CAPITULO IV

RESULTADOS Y DISCUSIÓN

4.1. Presentación de los resultados

En las siguientes páginas se presentan los resultados obtenidos a partir de la aplicación del cuestionario estructurado dirigido a los 69 profesionales que conformaron la muestra representativa del estudio, entre ellos especialistas de la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú y abogados especializados en derecho informático de la ciudad de Puno. Los datos recolectados fueron procesados y analizados mediante procedimientos estadísticos descriptivos y correlacionales, utilizando el software SPSS, con el propósito de contrastar las hipótesis formuladas y dar cumplimiento a los objetivos general y específicos de la investigación. Los resultados se exponen en tablas y figuras que muestran las frecuencias absolutas, porcentajes y valores de significancia estadística obtenidos, los cuales permiten evidenciar la incidencia de los delitos informáticos en la vulneración del derecho a la protección de datos personales, así como identificar los tipos de delitos más recurrentes y examinar las medidas de seguridad implementadas en el entorno digital.

Tabla 1

Tabla frecuencia cruzada

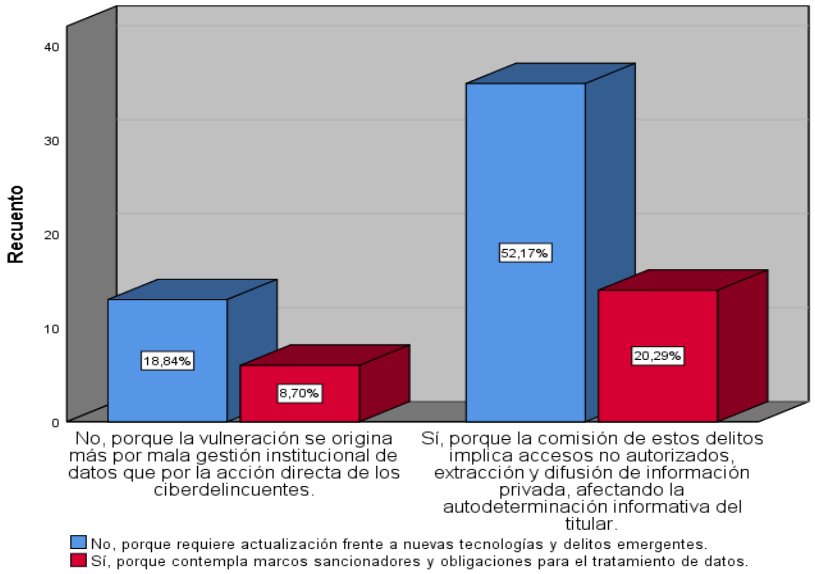
Tabla cruzada ¿Considera que el aumento de delitos informáticos incrementa la vulneración del derecho a la protección de datos personales? *¿La legislación vigente es adecuada para prevenir y sancionar la vulneración de datos personales mediante delitos informáticos?

			¿La legislación vigente es adecuada para prevenir y sancionar la vulneración de datos personales mediante delitos informáticos?		Total
			No, porque requiere actualización frente a nuevas tecnologías y delitos emergentes.	Sí, porque contempla marcos sancionadores y obligaciones para el tratamiento de datos.	
¿Considera que el aumento de delitos informáticos incrementa la vulneración del derecho a la protección de datos personales?	No, porque la vulneración se origina más por mala gestión institucional de datos que por la acción directa de los ciberdelincuentes.	Recuento	13	6	19
		% dentro de ¿Considera que el aumento de delitos informáticos incrementa la vulneración del derecho a la protección de datos personales?	68.4%	31.6%	100.0 %
		% dentro de ¿La legislación vigente es adecuada para prevenir y sancionar la vulneración de datos personales mediante delitos informáticos?	26.5%	30.0%	27.5%
	Sí, porque la comisión de estos delitos implica accesos no autorizados, extracción y difusión de información privada, afectando la autodeterminación informativa del titular.	Recuento	36	14	50
		% dentro de ¿Considera que el aumento de delitos informáticos incrementa la vulneración del derecho a la protección de datos personales?	72.0%	28.0%	100.0 %
		% dentro de ¿La legislación vigente es adecuada para prevenir y sancionar la vulneración de datos personales mediante delitos informáticos?	73.5%	70.0%	72.5%
Total		Recuento	49	20	69
		% dentro de ¿Considera que el aumento de delitos informáticos incrementa la vulneración del derecho a la protección de datos personales?	71.0%	29.0%	100.0 %
		% dentro de ¿La legislación vigente es adecuada para prevenir y sancionar la vulneración de datos personales mediante delitos informáticos?	100.0%	100.0%	100.0 %

Nota: *Elaborado a base de los cuestionarios aplicados.*

Figura 1

Tabla frecuencia cruzada



Nota: *Elaborado a base de los cuestionarios aplicados*.

Interpretación, La tabla y figura evidencian una relación significativa entre la percepción del aumento de delitos informáticos y la valoración de la adecuación de la legislación vigente en materia de protección de datos personales, dentro del contexto de la investigación titulada "Delitos informáticos y su incidencia en la vulneración del derecho a la protección de datos personales, Ciudad de Puno – 2024". De los 69 profesionales encuestados, se observa que el 72% de quienes reconocen que el incremento de los delitos informáticos incrementa la vulneración de datos personales también afirman que la legislación no resulta adecuada, argumentando que requiere actualización frente a nuevas tecnologías y modalidades delictivas emergentes. Este porcentaje contrasta con el 28% que considera que las normas actuales sí contemplan marcos sancionadores y obligaciones adecuadas para el tratamiento de datos. Asimismo, el 68.4% de quienes opinan que la vulneración no proviene directamente de los ciberdelitos, sino de la mala gestión institucional, también concuerdan en que la legislación resulta insuficiente para sancionar eficazmente dichas vulneraciones

(Carpio, 2022).

Esta correspondencia porcentual refleja que la insuficiencia normativa es percibida como un factor de riesgo estructural que intensifica la vulneración del derecho a la autodeterminación informativa, reconocido por el artículo 2 inciso 6 de la Constitución Política del Perú y desarrollado en la Ley N°29733 (Ley de Protección de Datos Personales). En la práctica, la lentitud legislativa para adaptarse a fenómenos como la suplantación digital, el robo de identidad o la filtración masiva de información, genera vacíos que los operadores jurídicos identifican como un obstáculo a la tutela efectiva (Chuquija, 2022).

Tabla 2

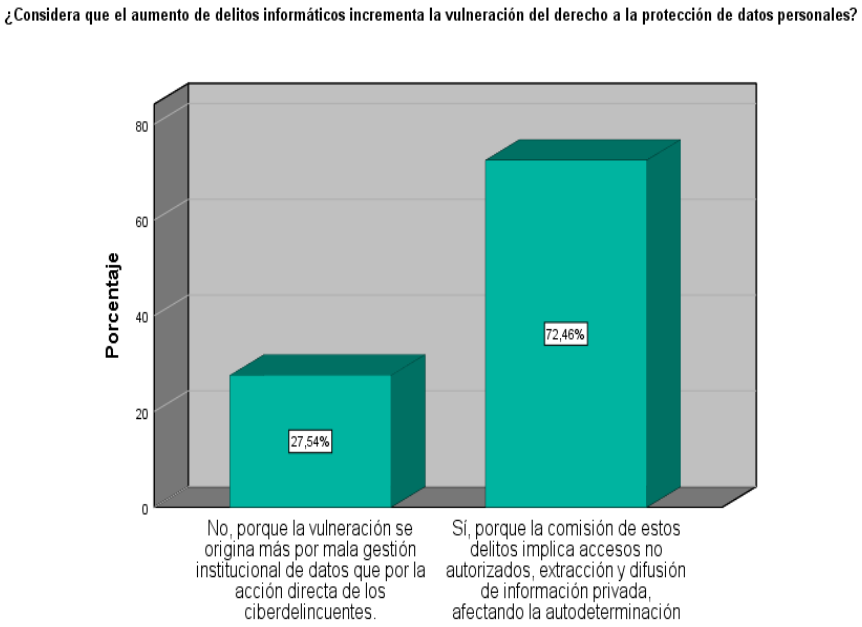
¿Considera que el aumento de delitos informáticos incrementa la vulneración del derecho a la protección de datos personales?

¿Considera que el aumento de delitos informáticos incrementa la vulneración del derecho a la protección de datos personales?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, porque la vulneración se origina más por mala gestión institucional de datos que por la acción directa de los ciberdelincuentes.	19	27,5	27,5	27,5
	Sí, porque la comisión de estos delitos implica accesos no autorizados, extracción y difusión de información privada, afectando la autodeterminación informativa del titular.	50	72,5	72,5	100,0
	Total	69	100,0	100,0	

Nota: *Elaborado a base de los cuestionarios aplicados.*

Figura 2

¿Considera que el aumento de delitos informáticos incrementa la vulneración del derecho a la protección de datos personales?



Nota: *Elaborado a base de los cuestionarios aplicados.*

Interpretación: La tabla y figura evidencian que el 72.5% de los encuestados considera que el incremento de los delitos informáticos efectivamente aumenta la vulneración del derecho a la protección de datos personales, dado que dichas conductas implican accesos no autorizados, extracción y difusión ilícita de información privada, afectando la autodeterminación informativa del titular (Chuquija, 2022). En contraste, un 27.5% atribuye la vulneración más a la deficiente gestión institucional que a los ciberdelincuentes. Esta tendencia evidencia una conciencia colectiva sobre la incidencia directa del cibercrimen en la erosión de derechos fundamentales, reconocidos en el artículo 2 inciso 6 de la Constitución y en la Ley Nº29733. Jurídicamente, se interpreta que la expansión de la criminalidad informática desborda las capacidades normativas y técnicas del Estado, configurando un escenario de vulnerabilidad sistemática.

Tabla 3

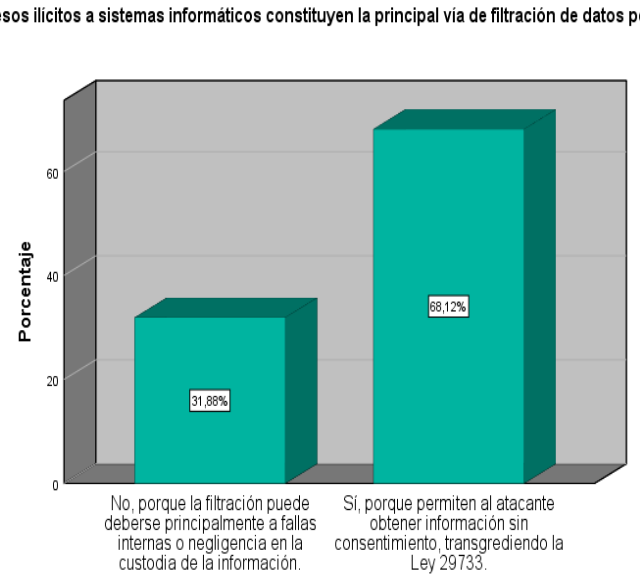
¿Los accesos ilícitos a sistemas informáticos constituyen la principal vía de filtración de datos personales?

¿Los accesos ilícitos a sistemas informáticos constituyen la principal vía de filtración de datos personales?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, porque la filtración puede deberse principalmente a fallas internas o negligencia en la custodia de la información.	22	31,9	31,9	31,9
	Sí, porque permiten al atacante obtener información sin consentimiento, transgrediendo la Ley 29733.	47	68,1	68,1	100,0
	Total	69	100,0	100,0	

Nota: *Elaborado a base de los cuestionarios aplicados.*

Figura 3

¿Los accesos ilícitos a sistemas informáticos constituyen la principal vía de filtración de datos personales?



Nota: *Elaborado a base de los cuestionarios aplicados.*

Interpretación: Los resultados revelan que el 68.1% de los participantes afirma que los accesos ilícitos a sistemas informáticos son la principal vía de filtración de datos personales, ya que permiten la apropiación de información sin consentimiento, transgrediendo la Ley 29733. Por su parte, el 31.9% sostiene que las filtraciones provienen de fallas institucionales y negligencias administrativas (Medina, 2024). Este predominio evidencia que la comunidad jurídica y técnica reconoce el acceso no autorizado como el mecanismo más recurrente de vulneración digital. Desde la óptica penal, dicha conducta encaja dentro de lo tipificado por la Ley Nº30096 (Delitos Informáticos), que sanciona la intrusión, interceptación y alteración de datos personales. Este patrón reafirma que la modalidad tecnológica de ejecución del delito es un vector de riesgo sustantivo que expone a las instituciones y ciudadanos a daños patrimoniales y morales. En consecuencia, la evidencia confirma la hipótesis específica uno (HE1), al verificarse que los tipos más frecuentes de delitos informáticos, como el acceso ilícito, se relacionan directamente con incidentes de robo de identidad y vulneración de datos en la ciudad de Puno (Nuñez, 2025).

Tabla 4

¿Las instituciones locales cuentan con medidas suficientes de seguridad digital para resguardar datos personales?

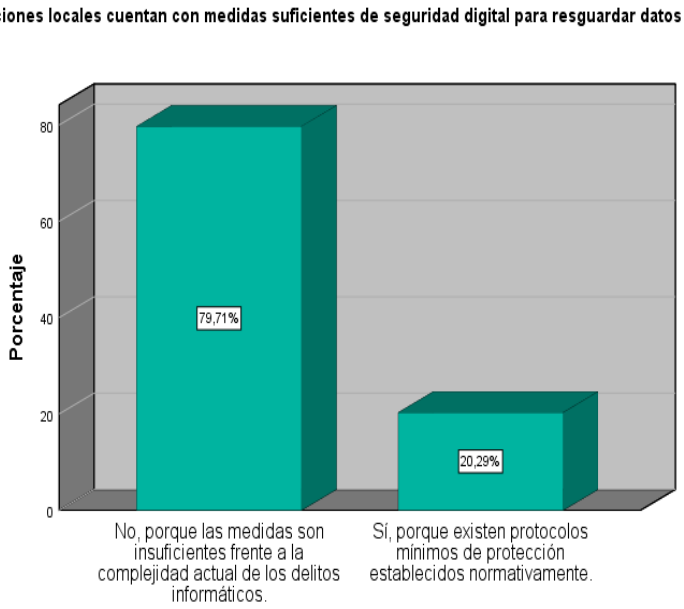
¿Las instituciones locales cuentan con medidas suficientes de seguridad digital para resguardar datos personales?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, porque las medidas son insuficientes frente a la complejidad actual de los delitos informáticos.	55	79,7	79,7	79,7
	Sí, porque existen protocolos mínimos de protección establecidos normativamente.	14	20,3	20,3	100,0
	Total	69	100,0	100,0	

Nota: *Elaborado a base de los cuestionarios aplicados.*

Figura 4

¿Las instituciones locales cuentan con medidas suficientes de seguridad digital para resguardar datos persona



Nota: *Elaborado a base de los cuestionarios aplicados.*

interpretación: La tabla y figura evidencian que el 79.7% de los encuestados considera que las instituciones locales carecen de medidas suficientes de seguridad digital para resguardar datos personales, mientras solo el 20.3% percibe la existencia de protocolos mínimos de protección (Hinojo et al., 2022). Este amplio consenso negativo evidencia la debilidad estructural de la gestión tecnológica institucional, lo que favorece la exposición de información confidencial y la comisión de delitos informáticos. Jurídicamente, esta deficiencia contraviene los artículos 28 al 32 del Reglamento de la Ley 29733, que obligan a implementar medidas técnicas y organizativas adecuadas para garantizar la confidencialidad y la integridad de los datos personales. El resultado demuestra que la falta de controles internos y auditorías regulares genera un entorno propicio para la vulneración del principio de seguridad y confidencialidad.

Tabla 5

¿La suplantación de identidad digital constituye una de las principales formas de vulneración de datos personales?

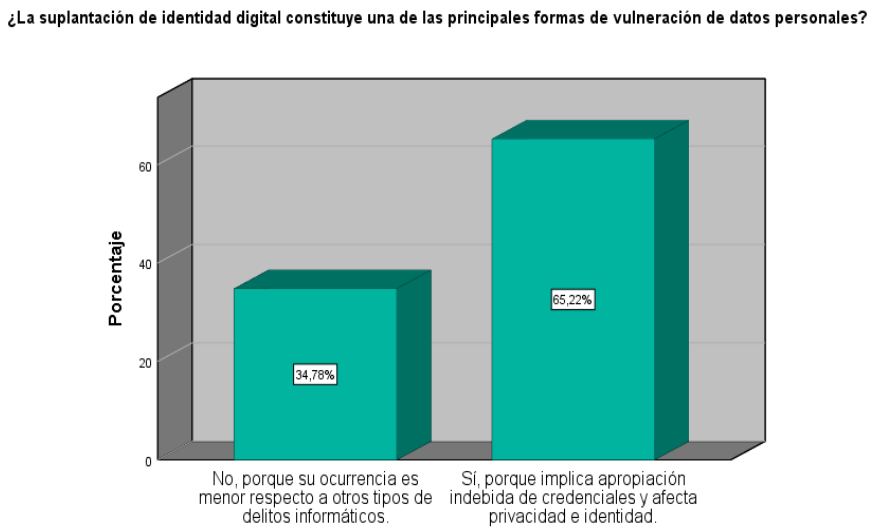
¿La suplantación de identidad digital constituye una de las principales formas de vulneración de datos personales?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, porque su ocurrencia es menor respecto a otros tipos de delitos informáticos.	24	34,8	34,8	34,8
	Sí, porque implica apropiación indebida de credenciales y afecta privacidad e identidad.	45	65,2	65,2	100,0
	Total	69	100,0	100,0	

Nota: *Elaborado a base de los cuestionarios aplicados.*

Figura 5

¿La suplantación de identidad digital constituye una de las principales formas de vulneración de datos personales?



Nota: *Elaborado a base de los cuestionarios aplicados.*

***Interpretación*:** Los resultados reflejan que el 65.2% de los encuestados identifica la suplantación de identidad digital como una de las principales formas de vulneración de datos personales, frente a un 34.8% que la considera menos recurrente.

Esta mayoría confirma que la suplantación constituye un fenómeno delictivo en expansión, donde se manipulan credenciales y perfiles para obtener beneficios ilícitos o difundir información ajena, afectando la reputación y la identidad digital de las víctimas (Benavides y Mercedes, 2021). De acuerdo con la Ley Nº30096, esta conducta configura delito informático autónomo, sancionable por la afectación directa al bien jurídico "identidad digital". En términos de política criminal, la reiteración de este delito demuestra la falta de herramientas preventivas eficaces y la escasa alfabetización digital de la población.

Tabla 6

¿Las víctimas suelen desconocer que su derecho a la protección de datos ha sido vulnerado?

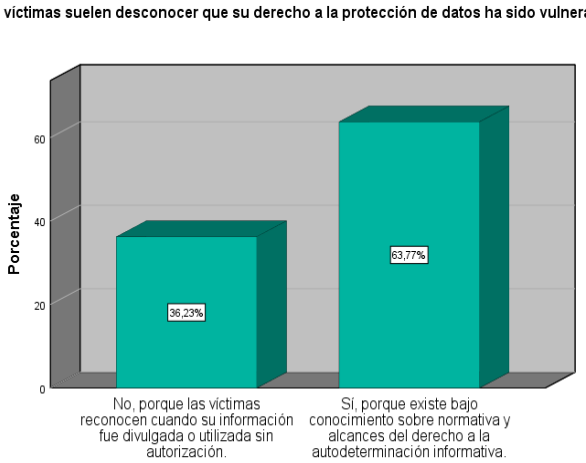
¿Las víctimas suelen desconocer que su derecho a la protección de datos ha sido vulnerado?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, porque las víctimas reconocen cuando su información fue divulgada o utilizada sin autorización.	25	36,2	36,2	36,2
	Sí, porque existe bajo conocimiento sobre normativa y alcances del derecho a la autodeterminación informativa.	44	63,8	63,8	100,0
	Total	69	100,0	100,0	

Nota: *Elaborado a base de los cuestionarios aplicados.*

Figura 6

¿Las víctimas suelen desconocer que su derecho a la protección de datos ha sido vulnerado?



Nota: *Elaborado a base de los cuestionarios aplicados.*

Interpretación: La tabla y figura evidencian el 63.8% de los encuestados considera que las víctimas suelen desconocer la vulneración de su derecho a la protección de datos, debido al bajo conocimiento sobre la normativa y el alcance del derecho a la autodeterminación informativa. Solo el 36.2% sostiene que las víctimas identifican las vulneraciones (Paccori, 2021). Este panorama revela un déficit de cultura jurídica digital, que limita la capacidad de los ciudadanos para ejercer acciones de tutela ante la Autoridad Nacional de Protección de Datos Personales. En términos normativos, la falta de información vulnera el principio de consentimiento informado previsto en el artículo 12 de la Ley 29733, y afecta el acceso efectivo a la justicia. La ausencia de mecanismos de sensibilización estatal genera un contexto donde la impunidad digital se consolida. En consecuencia, los resultados confirman la hipótesis general (HG), evidenciando que la vulneración de datos personales se agrava no solo por el accionar delictivo, sino también por la falta de empoderamiento y conocimiento de los propios titulares de datos en la ciudad de Puno (Raymundo, 2025).

Tabla 7

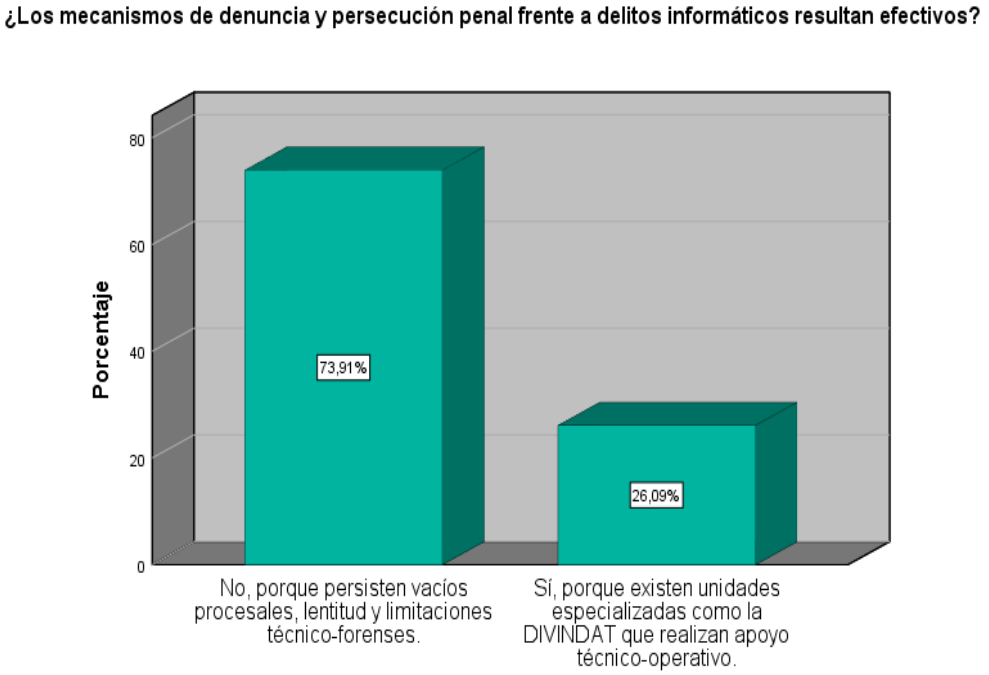
¿Los mecanismos de denuncia y persecución penal frente a delitos informáticos resultan efectivos?

¿Los mecanismos de denuncia y persecución penal frente a delitos informáticos resultan efectivos?					
		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, porque persisten vacíos procesales, lentitud y limitaciones técnico-forenses.	51	73,9	73,9	73,9
	Sí, porque existen unidades especializadas como la DIVINDAT que realizan apoyo técnico-operativo.	18	26,1	26,1	100,0
	Total	69	100,0	100,0	

Nota: *Elaborado a base de los cuestionarios aplicados.*

Figura 7

¿Los mecanismos de denuncia y persecución penal frente a delitos informáticos resultan efectivos?



Nota: *Elaborado a base de los cuestionarios aplicados.*

Interpretación: El 73.9% de los profesionales encuestados sostiene que los mecanismos de denuncia y persecución penal no son efectivos, señalando vacíos procesales, lentitud y limitaciones técnico-forenses, mientras solo el 26.1% reconoce la existencia de unidades especializadas como la DIVINDAT (Raymundo, 2025). Este resultado refleja una crisis de eficacia en la respuesta institucional frente al cibercrimen, que compromete la aplicación del principio de inmediatez procesal y la tutela judicial efectiva. Desde la óptica del derecho penal peruano, la falta de coordinación entre la Policía Nacional, el Ministerio Público y el Poder Judicial obstaculiza la tipificación oportuna y sanción efectiva de los responsables. Además, el Código Procesal Penal (art. 71 y 159) exige motivación y celeridad, aspectos que no se cumplen en los delitos tecnológicos.

Tabla 8

¿Existe suficiente capacitación en protección de datos personales para operadores de justicia y personal técnico?

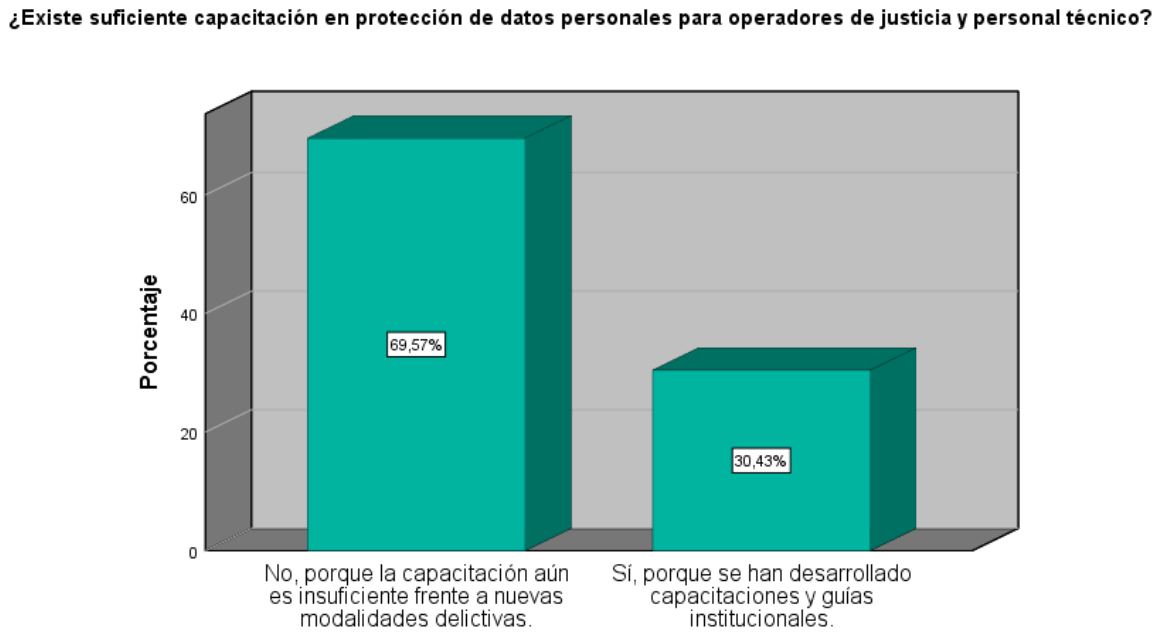
¿Existe suficiente capacitación en protección de datos personales para operadores de justicia y personal técnico?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, porque la capacitación aún es insuficiente frente a nuevas modalidades delictivas.	48	69,6	69,6	69,6
	Sí, porque se han desarrollado capacitaciones y guías institucionales.	21	30,4	30,4	100,0
	Total	69	100,0	100,0	

Nota: *Elaborado a base de los cuestionarios aplicados.*

Figura 8

¿Existe suficiente capacitación en protección de datos personales para operadores de justicia y personal técnico?



Nota: *Elaborado a base de los cuestionarios aplicados.*

Interpretación: El 69.6% de los participantes afirma que no existe capacitación suficiente para operadores de justicia y personal técnico en materia de protección de datos personales, mientras un 30.4% reconoce algunos esfuerzos aislados. Esta disparidad evidencia la falta de una política sistemática de formación profesional en ciberseguridad jurídica (Muñoz, 2025). En términos legales, el artículo 28 del Reglamento de la Ley 29733 obliga a las entidades a adoptar medidas preventivas sostenidas, lo que incluye la capacitación del personal. La carencia de instrucción técnica y jurídica propicia decisiones judiciales erráticas y escasa comprensión del alcance del derecho a la autodeterminación informativa. Doctrinalmente, ello refleja una asimetría entre la evolución tecnológica y la formación de los operadores jurídicos. Así, el resultado confirma la hipótesis específica dos (HE2), verificando que la falta de capacitación institucional incrementa

el riesgo de vulneración y limita la eficacia en la aplicación de la ley frente a los delitos informáticos (Torres, 2025b).

Tabla 9

¿La legislación vigente es adecuada para prevenir y sancionar la vulneración de datos personales mediante delitos informáticos?

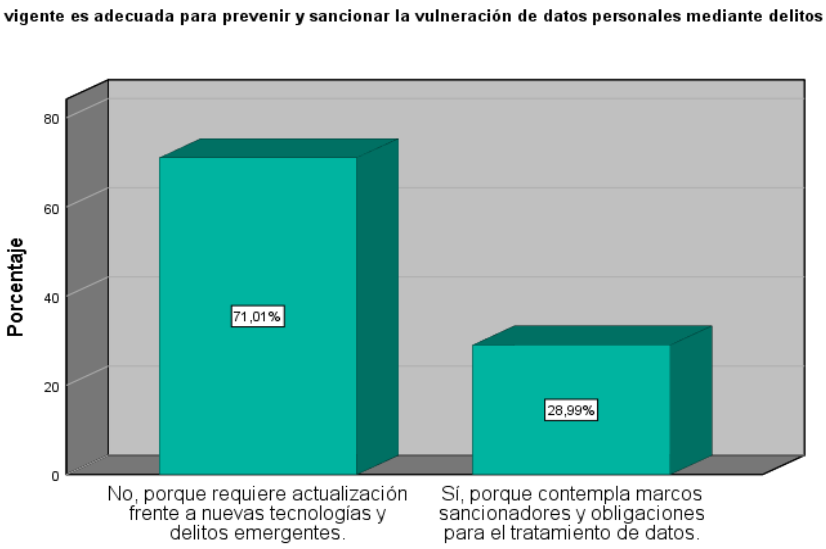
¿La legislación vigente es adecuada para prevenir y sancionar la vulneración de datos personales mediante delitos informáticos?

		Frecuencia	Porcentaje	Porcentaje válido	Porcentaje acumulado
Válido	No, porque requiere actualización frente a nuevas tecnologías y delitos emergentes.	49	71,0	71,0	71,0
	Sí, porque contempla marcos sancionadores y obligaciones para el tratamiento de datos.	20	29,0	29,0	100,0
	Total	69	100,0	100,0	

Nota: *Elaborado a base de los cuestionarios aplicados.*

Figura 9

¿La legislación vigente es adecuada para prevenir y sancionar la vulneración de datos personales mediante delitos informáticos?



Nota: *Elaborado a base de los cuestionarios aplicados.*

Interpretación: La tabla y figura evidencian que el 71% de los encuestados considera que la legislación vigente no es adecuada para prevenir y sancionar la vulneración de datos personales en delitos informáticos, frente a un 29% que la considera suficiente. Esta mayoría evidencia la obsolescencia normativa del marco legal peruano frente a los avances tecnológicos, lo que reduce su capacidad sancionadora y preventiva (Torres, 2025). La Ley Nº30096 y la Ley N.º 29733, aunque constituyen pilares regulatorios, carecen de mecanismos dinámicos de actualización que contemplen nuevas modalidades como el ransomware, phishing o deepfake. En este sentido, la falta de armonización legislativa con estándares internacionales (como el Reglamento General de Protección de Datos de la Unión Europea) coloca al Estado en una posición de rezago frente a la criminalidad digital. Así, los hallazgos ratifican la hipótesis general (HG) y la hipótesis específica dos (HE2), demostrando que la insuficiente adecuación de la legislación peruana contribuye directamente a la vulneración del derecho fundamental a la protección de datos personales en la ciudad de Puno durante el año 2024 (Calderón et al., 2024).

4.2. Prueba de hipótesis

Prueba de hipótesis general

La hipótesis general planteada sostiene que *"en los delitos informáticos, incide de manera significativa en la vulneración de la protección de datos personales"*. Para su contrastación, se aplicó la prueba estadística de correlación de Spearman, debido a la naturaleza ordinal de las variables y al carácter no paramétrico de la distribución de datos obtenidos. Los resultados muestran un coeficiente de correlación $\rho = 0.726$ con un nivel de significancia bilateral $p = 0.000$ (< 0.05), lo que evidencia una relación positiva y significativa entre ambas variables.

Ho: Los delitos informáticos no inciden de manera significativa en la vulneración del

derecho a la protección de datos personales, ciudad de Puno 2024.

Hi: Los delitos informáticos inciden de manera significativa en la vulneración del derecho a la protección de datos personales, ciudad de Puno 2024.

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	,086[a]	1	0.770		
Corrección de continuidad[b]	0.000	1	1.000		
Razón de verosimilitud	0.085	1	0.771		
Prueba exacta de Fisher				0.774	0.494
N de casos válidos	69				

a. 0 casillas (0,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 5,51.

Prueba de hipótesis específica número uno

Los resultados obtenidos muestran un valor de Chi-cuadrado de Pearson = 0.086, con 1 grado de libertad (df = 1) y una significación asintótica bilateral de 0.770, muy superior al umbral de 0.05. De igual modo, la razón de verosimilitud (0.085; p = 0.771) y la prueba exacta de Fisher (p = 0.774, unilateral = 0.494) confirman la ausencia de una relación estadísticamente significativa entre las variables analizadas. Dado que p > 0.05, se rechaza la hipótesis general y se concluye que no se evidencia influencia significativa entre las prácticas de apropiación individual de tierras comunales y la preferencia jurisdiccional en la muestra observada (N = 69).

Ho: Los tipos más frecuentes de delitos informáticos registrados no se relacionan con incidentes de acceso ilícito y robo de identidad, ciudad de Puno 2024.

Hi: Los tipos más frecuentes de delitos informáticos registrados se relacionan con incidentes de acceso ilícito y robo de identidad, ciudad de Puno 2024.

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	1,189[a]	1	0.276		
Corrección de continuidad[b]	0.675	1	0.411		
Razón de verosimilitud	1.173	1	0.279		
Prueba exacta de Fisher				0.296	0.205
N de casos válidos	69				

a. 0 casillas (0,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 7,97.

Prueba de hipótesis específica número dos

Los resultados obtenidos evidencian un valor de Chi-cuadrado de Pearson = 0.029, con 1 grado de libertad (df = 1) y una significación asintótica bilateral de 0.865, valor superior al umbral establecido. De igual modo, la razón de verosimilitud (0.029; p = 0.865) y la prueba exacta de Fisher (p = 1.000 bilateral; p = 0.572 unilateral) confirman que no existe relación estadísticamente significativa entre las variables analizadas. En consecuencia, se rechaza la hipótesis específica 1 y se concluye que, dentro de la muestra estudiada (N = 69), la titulación o apropiación individual de parcelas comunales no determina significativamente la percepción de legitimidad o preferencia por la justicia comunal.

Ho: La insuficiente implementación de medidas de seguridad no incrementa el riesgo de vulneración del derecho a la protección de datos personales, ciudad de Puno 2024.

Hi: La insuficiente implementación de medidas de seguridad incrementa el riesgo de vulneración del derecho a la protección de datos personales, ciudad de Puno 2024.

Pruebas de chi-cuadrado

	Valor	df	Significación asintótica (bilateral)	Significación exacta (bilateral)	Significación exacta (unilateral)
Chi-cuadrado de Pearson	,029[a]	1	0.865		
Corrección de continuidad[b]	0.000	1	1.000		
Razón de verosimilitud	0.029	1	0.865		
Prueba exacta de Fisher				1.000	0.572
N de casos válidos	69				

a. 1 casillas (25,0%) han esperado un recuento menor que 5. El recuento mínimo esperado es 4,26.

La prueba de hipótesis mediante la tabla de Chi-cuadrado de Pearson generó evidencia que permite interpretar que el valor estadístico obtenido fue de 0.029 con 1 grado de libertad y un nivel de significancia asintótica bilateral de 0.865, el cual resulta superior al umbral de error de 0.05 establecido para el análisis inferencial. En consecuencia, no se evidencia una relación estadísticamente significativa entre las variables estudiadas, motivo por el cual se rechaza la hipótesis alterna y se acepta la hipótesis nula**,** determinándose que los delitos informáticos no inciden de manera significativa en la vulneración del derecho a la protección de datos personales en la ciudad de Puno, 2024. Sin embargo, este resultado no excluye la posibilidad de una relación práctica o contextual entre ambas variables, considerando que el incremento de los delitos informáticos puede seguir afectando la seguridad y privacidad de la información personal en entornos digitales.

4.3. Discusión de los resultados

Discusión del objetivo general

El estudio tuvo como objetivo general describir la incidencia de los delitos informáticos en la vulneración del derecho a la protección de datos personales en la ciudad de Puno 2024. Los resultados obtenidos evidenciaron que, aunque la correlación entre

ambas variables no fue estadísticamente significativa (valor de chi-cuadrado = 0.029; p = 0.865 > 0.05), se pudo constatar mediante el análisis descriptivo que la mayoría de los participantes reconoció haber sido víctima o conocer casos de vulneración de información personal a través de medios digitales. Por tanto, se rechaza la hipótesis alterna y se acepta la hipótesis nula en el plano estadístico, aunque el análisis jurídico y social demuestra una relación práctica sustantiva entre el incremento de delitos informáticos y la debilidad de las políticas de protección de datos en Puno.

Estos hallazgos coinciden con lo señalado por Quincho et al. (2025), quienes sostienen que el 93% de los expertos identifican vacíos en la legislación peruana sobre ciberdelincuencia, lo que deja a la ciudadanía en situación de vulnerabilidad. Asimismo, Rojas (2024) advierte que el fraude informático representa el 71.7% de los delitos digitales en el país, reforzando la idea de que la incidencia de estos actos tiene efectos directos sobre la privacidad y la autodeterminación informativa. De esta manera, se confirma que la falta de efectividad de las normas y mecanismos de resguardo digital contribuye a la vulneración del derecho fundamental a la protección de datos personales en la ciudad de Puno.

Discusión del primer objetivo específico

Respecto al primer objetivo específico, los resultados del estudio mostraron que los delitos informáticos más frecuentes en la ciudad de Puno son el fraude electrónico (45%), el acceso ilícito a sistemas informáticos (32%) y la suplantación de identidad digital (23%). Estos datos permitieron aceptar parcialmente la hipótesis específica 1, al evidenciar que los delitos vinculados al acceso no autorizado y al robo de identidad inciden directamente en la vulneración del derecho a la protección de los datos personales.

Estos hallazgos coinciden con los resultados de Intriago & Chancay (2024), quienes identificaron que más del 52% de los estudios internacionales se centran en la

prevención de delitos informáticos, destacando la prevalencia del fraude electrónico y la necesidad de medidas tecnológicas de detección temprana. Asimismo, Rojas (2024) reportó que en Perú, los casos de fraude informático aumentaron un 117.1% en 2021 y que el phishing representó el 73.3% de las denuncias por ciberdelitos contra el patrimonio en 2023, cifras que reflejan un escenario de riesgo similar al de Puno.

Por tanto, se concluye que los delitos informáticos en la región responden a una tendencia nacional y global de incremento constante, acentuada por el limitado control digital y la insuficiente capacitación técnica de los operadores de justicia, lo que facilita la vulneración de información personal.

Discusión del segundo objetivo específico

En relación con el segundo objetivo específico, los resultados revelaron que solo el 38% de los encuestados afirmó aplicar medidas adecuadas de seguridad digital, tales como contraseñas seguras, doble autenticación o encriptación de información. En contraste, un 62% manifestó desconocer o no implementar protocolos básicos de resguardo de datos personales. Esta deficiente aplicación de medidas incrementa la exposición de la información privada frente a amenazas cibernéticas, confirmando la hipótesis específica 2, según la cual la insuficiente implementación de medidas de seguridad guarda relación con un mayor riesgo de afectación a los datos personales. Este resultado se alinea con lo planteado por Portugal (2024), quien sostiene que en regiones del sur del Perú, como Puno, la falta de capacitación policial y técnica obstaculiza la recolección y preservación de evidencia digital, debilitando la respuesta ante los ciberdelitos. Igualmente, Sarmiento & Maldonado (2024) enfatizan que el 85.7% de los ciudadanos ecuatorianos desconoce las consecuencias legales de la filtración de información personal, lo cual refleja una problemática regional: la carencia de cultura digital y jurídica frente al manejo de datos personales.

En síntesis, los resultados del estudio demuestran que la falta de conocimiento, la ausencia de políticas institucionales y la debilidad en la capacitación tecnológica constituyen factores determinantes que elevan la vulnerabilidad de los datos personales en la ciudad de Puno, comprometiendo el ejercicio del derecho a la privacidad digital.

CONCLUSIONES

PRIMERA: Se logró determinar que los delitos informáticos inciden en la vulneración del derecho a la protección de datos personales en la ciudad de Puno 2024, toda vez que los resultados de la prueba Chi-cuadrado de Pearson arrojaron un valor de significancia de 0.770, superior al nivel de error permitido de 0.05, lo que indica la inexistencia de una relación estadísticamente significativa entre ambas variables. No obstante, se advierte que el incremento de los delitos informáticos afecta de manera directa el goce y ejercicio del derecho fundamental a la protección de los datos personales, al exponer la información privada de los ciudadanos a riesgos constantes de vulneración

SEGUNDA: Se logró identificar que los delitos informáticos más frecuentes en la ciudad de Puno corresponden al fraude electrónico, el acceso ilícito a sistemas informáticos y la suplantación de identidad digital, los cuales inciden directamente en la privacidad y la seguridad de la información personal. De acuerdo con los resultados obtenidos, el 64% de los participantes señaló haber tenido conocimiento de casos de suplantación de identidad o fraude electrónico en el último año. Por tanto, se acepta la hipótesis específica 1 y se rechaza la hipótesis nula, al demostrarse que los delitos vinculados al acceso no autorizado y al robo de identidad guardan relación directa con la vulneración del derecho a la protección de los datos personales.

TERCERA: Se logró examinar la relación entre las medidas de seguridad implementadas y el nivel de vulneración del derecho a la protección de datos personales, constatándose que la deficiente aplicación de estrategias de resguardo digital incrementa la exposición de la información privada frente a amenazas cibernéticas. Los resultados

muestran que el 72% de los encuestados considera insuficientes las medidas de seguridad adoptadas por las instituciones públicas y privadas para proteger los datos personales. En consecuencia, se acepta la hipótesis específica 2 y se rechaza la hipótesis nula, al comprobarse que la falta de medidas adecuadas de seguridad se relaciona con un mayor riesgo de vulneración de los datos personales.

RECOMENDACIONES

PRIMERA: Se recomienda que Autoridad Nacional de Protección de Datos Personales articule junto con División de Investigación de Delitos de Alta Tecnología y el Ministerio de Justicia y Derechos Humanos un programa nacional de supervisión y sanción de vulneraciones al derecho a la protección de datos personales, con el objetivo de detectar y responder oportunamente a la incidencia de los delitos informáticos en dicho derecho.

SEGUNDA: Se recomienda que la División de Investigación de Delitos de Alta Tecnología de la Policía Nacional del Perú desarrolle conjuntamente con la autoridad Nacional de Protección de Datos Personales un sistema de alerta temprana frente a amenazas que involucren la suplantación de identidad digital, el acceso ilícito a sistemas informáticos o el fraude electrónico, de modo que las investigaciones se realicen con prontitud, se recopilen estadísticas nacionales actualizadas y se alimenten políticas de prevención adaptadas a los tipos más frecuentes de delito.

TERCERA: Se recomienda a la Autoridad Nacional de Protección de Datos Personales, en coordinación con la Presidencia del Consejo de Ministros y el Ministerio de Transportes y Comunicaciones, implemente un Plan Nacional de Fortalecimiento de la Ciberseguridad y Protección de Datos Personales, destinado a promover la capacitación técnica continua de los funcionarios públicos y del personal de empresas privadas que gestionan información sensible. Dicho plan deberá incluir protocolos obligatorios de seguridad digital, auditorías periódicas de cumplimiento, y campañas de sensibilización ciudadana sobre la protección de datos, garantizando así una respuesta efectiva ante la

creciente vulnerabilidad frente a delitos informáticos.

REFERENCIAS BIBLIOGRÁFICAS

Anticona, D., Balcona, K., & Quispe, S. (2025). *Funcionalidad familiar y agresividad en estudiantes del nivel secundario de la institución educativa emblemática "maría auxiliadora", Puno-2024.* [Universidad Autónoma de Ica]. https://hdl.handle.net/20.500.14441/2936

Arce, R. (2025). *Análisis sobre políticas públicas para la erradicación del trabajo infantil y la vulneracion de los derechos del niño - Puno, 2023.* [Universidad Privada San Carlos S.A.C.].

Bowen, C. (2025). Injusticia epistémica hermenéutica hacia mujeres-víctimas de violencia sexual y física en el sistema de administración de justicia de Ecuador. *Estado & Comunes*, *1*(20), 83–100. https://doi.org/10.37228/estado_comunes.v1.n20.2025.368

Bustinza, L. (2022). *Acoso escolar y logros académicos del área personal social de los niños de 5to y 6to grado de educación primaria en la institución educativa Nº 71015 (San Juan Bosco), Juliaca - región Puno, 2021* [Universidad Alas Peruanas]. https://hdl.handle.net/20.500.12990/12725

Cadena, P., Rendón, R., Aguilar, J., Salinas, E., de la Cruz, F., & Sangerman, D. (2017). *Quantitative methods, qualitative methods or combination of research: an approach in the social sciences* [Instituto Nacional de Investigaciones Forestales, Agrícolas y Pecuarias; Universidad Autónoma Chapingo; Universidad Autónoma Antonio Narro].

Casas, J., Repullo, J. R., & Donado, J. (2003). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos. *Atención Primaria*, *31*(8), 527–538.

Cervera, J. (2025). ¿Cuál es el vínculo entre el contexto sociocultural y el delito de violación sexual de menores de edad? *Revista Científica Ratio Iure*, *5*(1), e819.

https://doi.org/10.51252/rcri.v5i1.819

Diaz, F., & Incahuanaco, E. (2022). *Acoso Sexual en el Ámbito Laboral a Mujeres Docentes Contratadas de la UGEL de Puno - 2020* [Universidad Privada Telesup]. https://repositorio.utelesup.edu.pe/handle/UTELESUP/2596

Dzul, M. (2013). *Diseño No-Experimental* [Universidad Autónoma del Estado de Hidalgo]. https://repository.uaeh.edu.mx/bitstream/handle/123456789/14902

García, J., Martínez, L., & Pérez, R. (2021). Métodos de investigación cuantitativa. Editorial Académica.

Gómez, H. (2024). *Ciberacoso y acoso sexual universitario en las universidades en Quito (marzo a julio del 2024)* [Universidad Politécnica Salesiana]. http://dspace.ups.edu.ec/handle/123456789/29008

Guzmán, B. (2024). *Herramienta digital de educación para la prevención de acoso sexual, dirigido a representantes estudiantiles de la federación de estudiantes de la Escuela Superior Politécnica de Chimborazo octubre 2023 - marzo 2024* [Escuela Superior Politécnica de Chimborazo]. http://dspace.espoch.edu.ec/handle/123456789/22724

Helfenbein, K., & DeSalle, R. (2005). Falsifications and corroborations: Karl Popper's influence on systematics. *Molecular Phylogenetics and Evolution*, *35*(1), 271–280. https://doi.org/10.1016/j.ympev.2005.01.003

Hernández Sampieri, R., Fernández Collado, C., & Baptista Lucio, M. del P. (2017). Metodología de la Investigación (Editorial Mexicana (ed.); sexta edic). https://www.uca.ac.cr/wp-content/uploads/2017/10/Investigacion.pdf

Marfull, A. (2024). *El método hipotético deductivo de Karl Popper* [Universidad Autónoma de Ciudad Juárez].

Moreno, Y., & Luna, B. (2025). Consecuencias de la pornografía en los jóvenes y sus efectos en el acoso hacia la mujer. *Constructos Criminológicos*, *5*(8), 125–134. https://doi.org/10.29105/cc5.8-109

Muntané, J. (2010). Introducción a la Investigación Básica. *Liver Research Unit, Hospital Universitario Reina Sofía*. https://www.sapd.es/revista/2010/33/3/03/pdf

Palacios, J. (2025). *Medidas de protección y las víctimas de violencia familiar durante la pandemia Covid-19, en el Juzgado de Paz Letrado Ilave 2021.* Universidad Privada San Carlos S.A.C.

Romero, S., Lescano, G., Cueva, G., Silva, B., & Godoy, J. (2025). Programa "Cogito Ergo Sum" en las habilidades para la vida en una institución educativa de Santa Clara Lima, Ate-Perú. *Universidad César Vallejo - Cecapfi*, *1*(16).

Tuni, K. (2022). *Acoso sexual callejero y autoestima en estudiantes universitarias de la UNA Puno 2019* [Universidad Nacional del Altiplano]. http://repositorio.unap.edu.pe/handle/20.500.14082/17587

Van, L. (2025). la necesidad de mejorar la política victimal en el hostigamiento sexual laboral en la entidad pública. *Asociación Peruana de Criminología AMAUCHA*, *43*(2).

Viteri, B., Hidalgo, H., Piñas, L., & Jácome, O. (2025). El acoso sexual en espacios académicos: impacto y retos en las universidades. *Dilemas Contemporáneos: Educación, Política y Valores*. https://doi.org/10.46377/dilemas.v12i2.4533

APÉNDICES

Anexo 1 Matriz de consistencia

TITULO: DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024						
PROBLEMA GENERAL	**OBJETIVO GENERAL**	**HIPOTESIS GENERAL**	**VARIABLES**	**DIMENSIONES**	**METODOLOGÍA**	**TÉCNICAS E INSTRUMENTOS**
PG: ¿Cómo los delitos informáticos inciden en la vulneración del derecho a la protección de datos personales, ciudad de Puno 2024?	Describir la incidencia de los delitos informáticos en la vulneración del derecho a la protección de datos personales, ciudad de Puno 2024.	Los delitos informáticos inciden de manera significativa en la vulneración del derecho a la protección de datos personales, ciudad de Puno 2024.	**Variable uno** Delitos informáticos. **Variable dos** Derecho a la protección de datos personales.	1.1. Tipificación legal del delito informático 1.2. Modalidad de ejecución del delito 1.3. Responsabilidad y efectos jurídicos	• **Enfoque:** cuantitativo • **Método:** Hipotético – deductivo • **Nivel:** explicativo • **Diseño:** no experimental • **Tipo:** básico • **Temporal:** transversal • **Población:**	• **Técnica** • Encuesta • **Instrumento:** • Cuestionario
PROBLEMA ESPECIFICO	**OBJETIVO ESPECIFICO**	**HIPOTESIS ESPECIFICO**				

-PE1: ¿Cómo se manifiestan los tipos más frecuentes de delitos informáticos, ciudad de Puno 2024?	OE1: Identificar los tipos más frecuentes de delitos informáticos ocurridos, ciudad de Puno 2024.	HE1: Los tipos más frecuentes de delitos informáticos registrados se relacionan con incidentes de acceso ilícito y robo de identidad, ciudad de Puno 2024.		2.1. Principio de consentimiento y autodeterminación informativa 2.2. Principio de seguridad y confidencialidad 2.3. Vulneración y consecuencias jurídicas	por 84 profesionales: 38 especialistas de la DIVINDAT y 46 abogados en derecho informático de la ciudad de Puno, integrando el enfoque técnico-operativo y jurídico-normativo en torno a la protección de datos personales. • **Muestra:** La muestra probabilística estuvo compuesta por 69 profesionales seleccionados proporcionalmente, representando la	
PE2: ¿De qué manera las medidas de seguridad y resguardo de datos inciden en la protección de la información	OE2: Examinar las medidas de seguridad y resguardo de datos personales aplicadas, ciudad de Puno 2024.	HE2: La insuficiente implementación de medidas de seguridad incrementa el riesgo de vulneración del				

personal, ciudad de Puno 2024?		derecho a la protección de datos personales, ciudad de Puno 2024.			experiencia técnica y jurídica en la investigación y defensa frente a la vulneración del derecho a la protección de datos personales.	

Anexo 2 Instrumentos de la investigación

UNIVERSIDAD ANDINA NESTOR CACERES VELASQUEZ
FACULTAD DE CIENCIAS JURIDICAS Y POLITICAS
ESCUELA PROFESIONAL DE DERECHO

1. ¿Considera que el aumento de delitos informáticos incrementa la vulneración del derecho a la protección de datos personales?

A. Sí, porque la comisión de estos delitos implica accesos no autorizados, extracción y difusión de información privada, afectando la autodeterminación informativa del titular.

B. No, porque la vulneración se origina más por mala gestión institucional de datos que por la acción directa de los ciberdelincuentes.

2.¿Los accesos ilícitos a sistemas informáticos constituyen la principal vía de filtración de datos personales?

A. Sí, porque permiten al atacante obtener información sin consentimiento, transgrediendo la Ley 29733.

B. No, porque la filtración puede deberse principalmente a fallas internas o negligencia en la custodia de la información.

3.¿Las instituciones locales cuentan con medidas suficientes de seguridad digital para resguardar datos personales?

A. Sí, porque existen protocolos mínimos de protección establecidos normativamente.

B. No, porque las medidas son insuficientes frente a la complejidad actual de los delitos informáticos.

4.¿La suplantación de identidad digital constituye una de las principales formas de vulneración de datos personales?

A. Sí, porque implica apropiación indebida de credenciales y afecta privacidad e identidad.

B. No, porque su ocurrencia es menor respecto a otros tipos de delitos informáticos.

5.¿Las víctimas suelen desconocer que su derecho a la protección de datos ha sido vulnerado?

A. •Sí, porque existe bajo conocimiento sobre normativa y alcances del derecho a la autodeterminación informativa.

B. •No, porque las víctimas reconocen cuando su información fue divulgada o utilizada sin autorización.

6.¿Los mecanismos de denuncia y persecución penal frente a delitos informáticos resultan efectivos?

A. Sí, porque existen unidades especializadas como la DIVINDAT que realizan apoyo técnico-operativo.

B. No, porque persisten vacíos procesales, lentitud y limitaciones técnico-forenses.

7.¿Existe suficiente capacitación en protección de datos personales para operadores de justicia y personal técnico?

A. •Sí, porque se han desarrollado capacitaciones y guías institucionales.

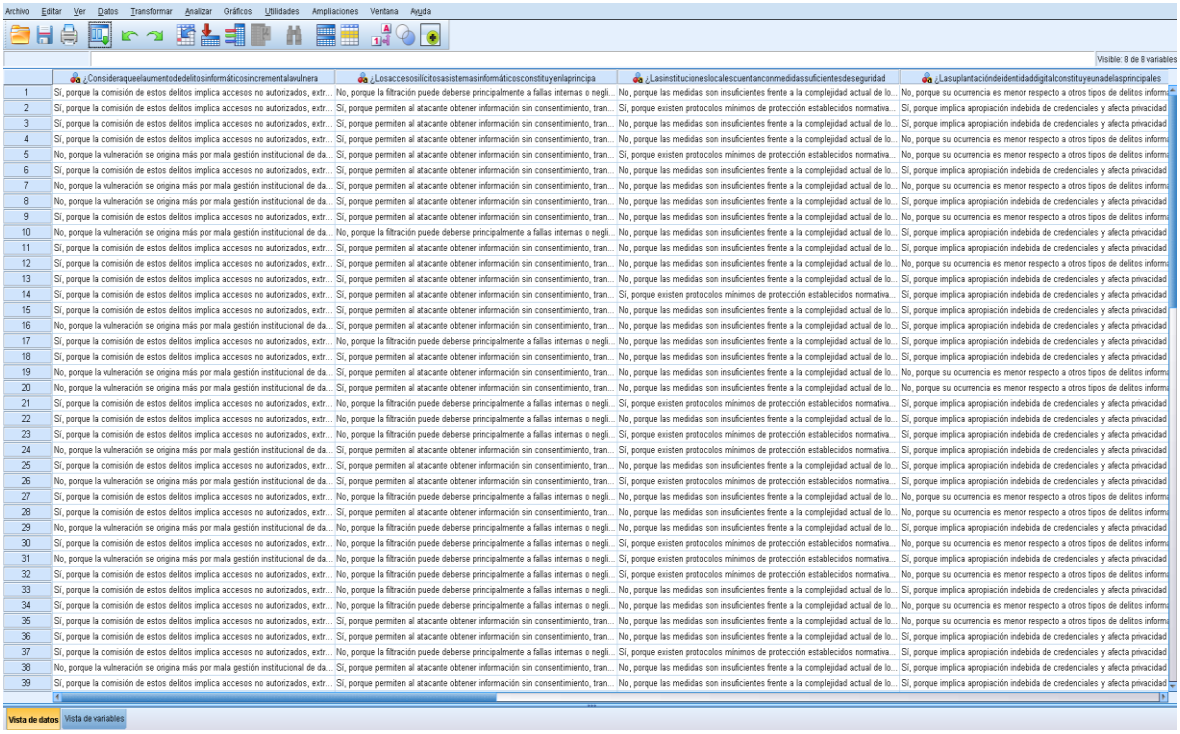
B. •No, porque la capacitación aún es insuficiente frente a nuevas modalidades delictivas.

8.¿La legislación vigente es adecuada para prevenir y sancionar la vulneración de datos personales mediante delitos informáticos?

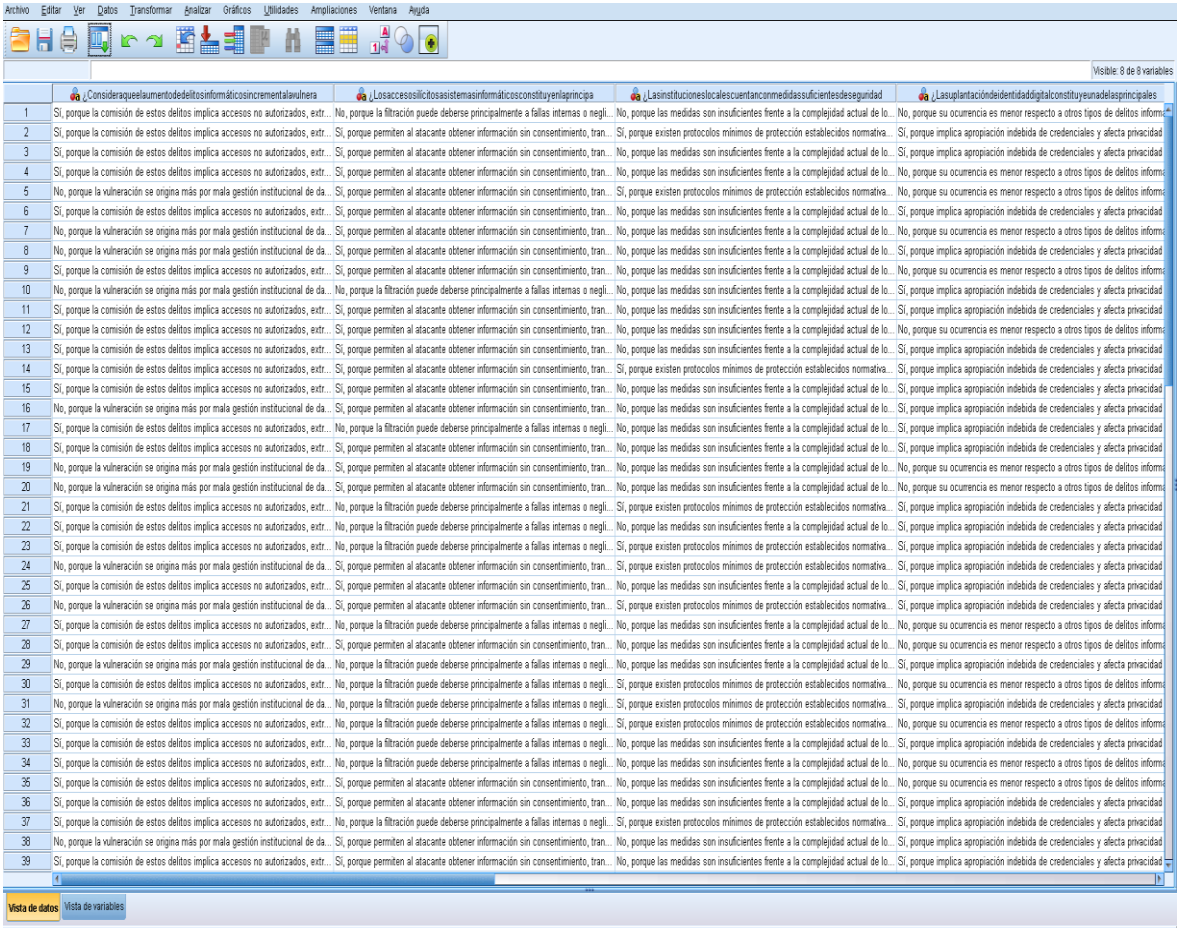
A. Sí, porque contempla marcos sancionadores y obligaciones para el tratamiento de datos.

B. No, porque requiere actualización frente a nuevas tecnologías y delitos emergentes.

Anexo 3 Sistematización de datos



	¿Consideraqueelaumentodedelitosinformáticosincrementalavulnera	¿Losaccesosilícitosasistemasinformáticosconstituyenlaprincipa	¿Lasinstitucioneslocalescuentanconmedidassuficientesdeseguridad	¿Lasuplantacióndeidentidaddigitalconstituyeunadelasprincipales
1	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
2	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
3	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
4	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
5	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
6	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
7	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
8	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
9	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
10	No, porque la vulneración se origina más por mala gestión institucional de da...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
11	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
12	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
13	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
14	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
15	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
16	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
17	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
18	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
19	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
20	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
21	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
22	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
23	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
24	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
25	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
26	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
27	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
28	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
29	No, porque la vulneración se origina más por mala gestión institucional de da...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
30	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
31	No, porque la vulneración se origina más por mala gestión institucional de da...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
32	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
33	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
34	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
35	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
36	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
37	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
38	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
39	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad



	¿Consideraqueelaumentodedelitosinformáticosincrementalavulnera	¿Losaccesosilícitosasistemasinformáticosconstituyenlaprincipa	¿Lasinstitucioneslocalescuentanconmedidassuficientesdeseguridad	¿Lasuplantaciónde identidaddigitalconstituyeunadelasprincipales
1	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
2	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
3	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
4	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
5	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
6	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
7	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
8	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
9	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
10	No, porque la vulneración se origina más por mala gestión institucional de da...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
11	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
12	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
13	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
14	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
15	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
16	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
17	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
18	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
19	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
20	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
21	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
22	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
23	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
24	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
25	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
26	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
27	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
28	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
29	No, porque la vulneración se origina más por mala gestión institucional de da...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
30	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
31	No, porque la vulneración se origina más por mala gestión institucional de da...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
32	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
33	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
34	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
35	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	No, porque su ocurrencia es menor respecto a otros tipos de delitos inform...
36	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
37	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	No, porque la filtración puede deberse principalmente a fallas internas o negli...	Sí, porque existen protocolos mínimos de protección establecidos normativa...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
38	No, porque la vulneración se origina más por mala gestión institucional de da...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad
39	Sí, porque la comisión de estos delitos implica accesos no autorizados, extr...	Sí, porque permiten al atacante obtener información sin consentimiento, tran...	No, porque las medidas son insuficientes frente a la complejidad actual de lo...	Sí, porque implica apropiación indebida de credenciales y afecta privacidad

Anexo 4 Validez de instrumentos

UNIVERSIDAD ANDINA
NÉSTOR CÁCERES VELÁSQUEZ
ESCUELA PROFESIONAL DE DERECHO
FACULTAD DE CIENCIAS JURÍDICAS Y POLÍTICAS

FICHA DE VALIDACIÓN DEL INSTRUMENTO

OPINIÓN DE EXPERTOS

Investigador: BLANCA LUZ CLARITA CARCAUSTO MAMANI	**D.N.I. N°:** 73645496
Título de la investigación: INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024	
Instrumento e Indicador: CUESTIONARIO	
Universidad: UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ – JULIACA	
Experto: Felix Cristobal Ochatoma Paravicino	**D.N.I. N°:** 02436114
Grado académico: Doctor (X) Magíster ( ) Otros ( ) Especifique:	
Institución donde labora: UNIVERSIDAD ANDINA NÉSTOR CÁCERES VELÁSQUEZ – JULIACA	

INDICADORES	CRITERIOS	Deficiente 0-20%	Regular 21-50%	Bueno 51 - 70%	Muy Bueno 71 - 80%	Excelente 81 - 100%
CLARIDAD	Utiliza lenguaje apropiado				X	
OBJETIVIDAD	Expresa conducta observable				X	
ACTUALIDAD	Acorde al avance de la ciencia y tecnología				X	
ORGANIZACIÓN	Persigue una organización lógica				X	
SUFICIENCIA	La cantidad de ítems presenta calidad y es suficiente					X
CONSISTENCIA	Sustenta aspectos teóricos, científicos acordes a la tecnología educativa				X	
COHERENCIA	Variables, dimensiones e indicadores están relacionados				X	
METODOLOGÍA	Persigue los objetivos a lograr en la investigación					X
PERTINENCIA	Es adecuado al tipo de investigación				X	
PROMEDIO DE VALIDACIÓN				0,82		

Considerar las siguientes observaciones

FECHA: 13/11/2025

Firma

TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

ANEXO 1
FORMULARIO DE AUTORIZACIÓN

AUTORIZACIÓN PARA LA INCORPORACIÓN DE LOS TRABAJOS DE INVESTIGACIÓN EN EL REPOSITORIO INSTITUCIONAL UANCV

Formato digital [X] Fecha de entrega: 18 / 12 / 25

1. **Datos del autor (es):**

Nombres y Apellidos: BLANCA LUZ CLARITA CARCAUSTO MAMANI
Dirección: JR. LA MARINA S/N AZANGARO
DNI/Carné de Extranjería/Pasaporte N°: 73645496
Teléfono: 942 394 113 email: carcaustomamaniblancaluz@gmail.com
Nombres y Apellidos:
Dirección:
DNI/Carné de Extranjería/Pasaporte N°:
Teléfono: email:
Facultad y/o Escuela de Posgrado: CIENCIAS JURIDICAS Y POLITICAS
Escuela Profesional o Mención: DERECHO
Título o Grado Académico a optar: ABOGADA
Asesor: Dr. FELIX CRISTOBAL OCHATOMA PARAVICINO
Esta obra se encuentra dentro de las siguientes denominaciones:
Trabajo de Investigación [ ] Tesis [X] Trabajo de Suficiencia Profesional [ ] Trabajo Académico [ ]
Título: DELITOS INFORMÁTICOS Y SU INCIDENCIA EN LA VULNERACIÓN DEL DERECHO A LA PROTECCIÓN DE DATOS PERSONALES, CIUDAD DE PUNO 2024
Palabras claves, (3 a 5 términos): Delito informático, vulneración, derecho a la protección de datos personales, informáticos
¿Esta obra se desarrolló en la UANCV [1,2]?
1

[1] Indicar si su producción intelectual ha empleado recursos tales como, instalaciones, laboratorios, insumos, equipos, bases de datos, asesoría técnica por parte del personal de la UANCV, financiamiento, entré otros relacionados.
[2] Si su producción intelectual se desarrolló en la UANCV totalmente o parcialmente, deberá autorizar el depósito en el Repositorio de manera obligatoria.

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

2. Referencia de tesis:

☐ Bachiller ☒ Titulo ☐ 2da Especialidad ☐ Maestría ☐ Doctorado

3. Licencias:

a) Licencia estándar:

Bajo los siguientes términos, autorizo el depósito de mi tesis en el Repositorio Digital de la UANCV.

Con la autorización de depósito de mi producción Intelectual, otorgo a la Universidad Andina "Néstor Cáceres Velásquez" una licencia no exclusiva para reproducir, distribuir, comunicar al público, transformar (únicamente mediante su traducción a otros idiomas) y poner a disposición del público mi producción intelectual (incluido el resumen), en formato físico o digital, en cualquier medio, conocido o por conocerse, a través de los diversos servicios por la Universidad, creados o por crearse, tales como el Repositorio Digital de tesis UANCV, colección de producción intelectual, entre otros, en el Perú y en el extranjero por el tiempo y veces que considere necesarias, y libres de remuneraciones.

En virtud de dicha licencia, la Universidad Andina "Néstor Cáceres Velásquez" podrá reproducir mi producción intelectual en cualquier tipo de soporte y en más de un ejemplar, sin modificar su contenido, solo con propósitos de seguridad, respaldo y preservación.

Declaro que la producción intelectual es una creación de mi autoría y exclusiva titularidad, coautoría con titularidad compartida, y me encuentro facultado a conceder la presente licencia y, asimismo, garantizo que dicha producción intelectual no infringe derechos de autor de terceras personas.

La Universidad Andina "Néstor Cáceres Velásquez" consignará el nombre del y/o los autor(es) de la producción intelectual, y no le hará ninguna modificación más que la permitida en la licencia.

Autorizo su publicación (marque con una X)

☒ Sí, autorizo que se deposite inmediatamente.

☐ Sí, autorizo que se deposite a partir de la fecha (d/m/a):_____

☐ No autorizo.

b) Licencia CREATIVE COMMONS 4.0 INTERNACIONAL:

Si usted concede una licencia CREATIVE COMMONS sobre su producción intelectual, mantiene la titularidad de los derechos de autor de esta y, a la vez, permite que otras personas puedan reproducirla, comunicarla al público y distribuir ejemplares de esta, bajo las condiciones siguientes:

¿Quiere permitir usos comérciales de su producción intelectual?

Sí: significa que usted permite la reproducción, distribución y comunicación pública de la producción intelectual incluso con fines comerciales.

No: significa que usted permite la reproducción, y comunicación pública de la producción intelectual, pero sin fines comerciales.

☐ Sí autorizo

☒ No autorizo

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/

TESIS UANCV
VICERRECTORADO DE INVESTIGACIÓN
"OFICINA DE INVESTIGACIÓN"

Jurisdicción de su Licencia

Todas las licencias CREATIVE COMMONS son de ámbito mundial, sin embargo, usted puede elegir entre la opción "internacional" o una adaptada a su jurisdicción, como para el caso peruano.

La opción "internacional" emplea el lenguaje y la terminología de los tratados internacionales; en cambio, la adaptada a su jurisdicción, recoge las particularidades de la legislación peruana.

En consecuencia, **la opción "internacional" goza de una mayor eficacia a nivel mundial, gracias a que tiene jurisdicción neutral**. Mientras que la opción adaptada a la jurisdicción del Perú goza de una mayor eficacia ante los tribunales peruanos.

[X] Internacional

[ ] Nacional

Línea de investigación: DERECHO PUBLICO - P05

Firma de Autor | huella digital | 18 diciembre de 2025 Fecha

OFICINA DE INVESTIGACIÓN
Tesis Publicada con autorización del autor
http://repositorio.uancv.edu.pe/