

UNIVERSIDAD PERUANA DE CIENCIAS E INFORMÁTICA
FACULTAD DE DERECHO Y CIENCIAS POLÍTICAS
CARRERA PROFESIONAL DE DERECHO



TRABAJO DE SUFICIENCIA PROFESIONAL

“Análisis crítico de la regulación de los delitos informáticos en el
Código Penal Peruano”

AUTOR:

Bach. Aduviri Flores, José Carlos

PARA OPTAR EL TÍTULO PROFESIONAL DE:
ABOGADO

ASESOR:

Dr. Castillo Figueroa, Carlos Francisco

ORCID: 0009-0009-6953-651X

DNI: 09530087

LIMA-PERÚ

2025

INFORME DE SIMILITUD

N°083-2025-UPCI-FDCP-REHO-T

A : **MG. HERMOZA OCHANTE RUBEN EDGAR**
Decano (e) de la Facultad de Derecho y Ciencias Políticas

DE : **MG. HERMOZA OCHANTE, RUBEN EDGAR**
Docente Operador del Programa Turnitin

ASUNTO : Informe de evaluación de Similitud de Trabajo de Suficiencia Profesional:
BACHILLER ADUVIRI FLORES, JOSE CARLOS

FECHA : Lima, 24 de noviembre de 2025.

Tengo el agrado de dirigirme a usted con la finalidad de informarle lo siguiente:

1. Mediante el uso del programa informático **Turnitin** (con las configuraciones de excluir citas, excluir bibliografía y excluir oraciones con cadenas menores a 20 palabras) se ha analizado el Trabajo de Suficiencia Profesional titulada: "**ANÁLISIS CRÍTICO DE LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL PERUANO**", presentado por el Bachiller **ADUVIRI FLORES, JOSE CARLOS**.
2. Los resultados de la evaluación concluyen que el Trabajo de Suficiencia Profesional en mención tiene un **ÍNDICE DE SIMILITUD DE 11%** (cumpliendo con el artículo 35 del Reglamento de Grado de Bachiller y Título Profesional UPCI aprobado con Resolución N° 373-2019-UPCI-R de fecha 22/08/2019).
3. Al término análisis, el Bachiller en mención **PUEDE CONTINUAR** su trámite ante la facultad, por lo que el resultado del análisis se adjunta para los efectos consiguientes

Es cuanto hago de conocimiento para los fines que se sirva determinar.

Atentamente,


.....
MG. HERMOZA OCHANTE, RUBEN EDGAR
Universidad Peruana de Ciencias e Informática
Docente Operador del Programa Turnitin

Adjunto:

**Resultado de similitud*

Dedicatoria

El presente trabajo se lo dedico a mis padres, dado que ellos son la fuerza que me empuja hacia adelante para continuar sembrando logros a lo largo de mi vida.

Agradecimiento

Quiero agradecer a mi alma mater y a sus autoridades; a mis maestros y a mis compañeros de clase, por sus consejos y buen ánimo para apoyarme y darme fuerza durante toda mi formación académica.

Declaración de Autoría

Nombres : José Carlos

Apellidos : Aduviri Flores

Código : 1401000420

DNI : 45432539

Declaro que, soy el autor del trabajo realizado y que es la versión final que he entregado a la oficina del Decanato de la Facultad de Derecho y Ciencias Políticas de la Universidad Peruana de Ciencias e Informática.

Asimismo, declaro que he citado debidamente las palabras o ideas de otros autores, refiriendo expresamente el nombre de la obra y página o páginas que me sirvieron de fuente.

Jesús María, 31 octubre del 2025.

ÍNDICE

CARATULA.....	1
INFORME DE SIMILITUD.....	2
DEDICATORIA.....	3
AGRADECIMIENTO.....	4
DECLARACIÓN DE AUTORÍA.....	5
ÍNDICE.....	6
INTRODUCCIÓN.....	7
CAPITULO I: Planificación del Trabajo de Suficiencia Profesional	9
1.1. Título y descripción del trabajo	9
1.2. Objetivo del trabajo	9
1.3. Justificación	12
CAPITULO II: Marco Teórico.....	17
2.1. Definición y clasificación de los delitos informáticos.....	17
2.2. Evolución histórica de la regulación de los delitos informáticos a nivel internacional y nacional	23
CAPITULO III: Desarrollo de actividades programadas.....	28
3.1. Identificación de vacíos, ambigüedades o deficiencias en la regulación actual	28
3.2. Opinión doctrinaria sobre la eficacia de la normativa vigente	33
CAPITULO IV: Resultados Obtenidos.....	37
CONCLUSIONES	39
RECOMENDACIONES	41
REFERENCIAS BIBLIOGRÁFICAS.....	43
ANEXOS.....	48
Anexo 1: Evidencia de similitud digital.....	48
Anexo 2: Autorización de publicación en repositorio.....	52

INTRODUCCION

En la actualidad, el vertiginoso avance de las tecnologías de la información y la comunicación se ha transformado radicalmente de la manera en que las personas interactúan, acceden a la información y realizan actividades económicas, sociales y culturales; sin embargo, este desarrollo tecnológico también ha propiciado la aparición de nuevas formas de criminalidad, conocidas como delitos informáticos, que desafiaban los marcos jurídicos tradicionales y exigen respuestas normativas especializadas; en ese sentido, los delitos informáticos, entendidos como aquellas conductas ilícitas que se cometen mediante el uso de sistemas informáticos o que tienen como objetos bienes jurídicos vinculados a la información digital, presentan características particulares, como su dimensión transnacional, la sofisticación técnica de los autores y la dificultad para su persecución y sanción.

En el contexto peruano, la regulación de los delitos informáticos ha experimentado una evolución significativa en las últimas décadas. Inicialmente, el Código Penal peruano abordó estos ilícitos de manera limitada, considerándolos en algunos casos como modalidades agravadas de delitos tradicionales, como el hurto; no obstante, la creciente complejidad y frecuencia de estos delitos motivó la promulgación de normas específicas, como la Ley N° 30096, que tipifica y sanciona diversas conductas delictivas relacionadas con el uso indebido de tecnologías de la información.

A pesar de estos avances, persisten cuestionamientos sobre la suficiencia, claridad y eficacia de la regulación vigente, así como sobre la adecuación de las figuras penales a la realidad tecnológica y social actual.

El presente trabajo tiene como objetivo realizar un análisis crítico de la regulación de los delitos informáticos en el Código Penal peruano, identificando sus principales aciertos y deficiencias, y proponiendo alternativas para su mejora; para ello, se examinarán los fundamentos doctrinarios y normativos de la materia, se analizarán casos emblemáticos y se evaluará la respuesta del sistema penal frente a los desafíos que plantea la criminalidad informática en el Perú, de esta manera, se busca contribuir al debate académico y legislativo sobre la necesidad de contar con un marco jurídico adecuado y efectivo para la prevención y sanción de los delitos informáticos en nuestro país.

CAPITULO I.- Planificación del Trabajo de Suficiencia Profesional

1.1. Título y descripción del trabajo

Título del Trabajo

La presente investigación la he denominado: Análisis crítico de la regulación de los delitos informáticos en el Código Penal peruano.

1.2. Objetivo del presente trabajo

El cumplimiento de estos objetivos permitirá no solo una comprensión integral del estado actual de la regulación de los delitos informáticos en el Perú, sino también la identificación de vacíos normativos y desafíos prácticos que afectan la eficacia del sistema penal; asimismo, contribuirá al debate académico y legislativo sobre la necesidad de adaptar el Derecho Penal a las nuevas realidades tecnológicas, garantizando una protección

adecuada frente a la ciberdelincuencia y promoviendo un equilibrio entre seguridad y derechos fundamentales.

Objetivo general

El objetivo principal de la presente tesis es realizar un análisis crítico de la regulación de los delitos informáticos en el Código Penal peruano, evaluando su eficacia, coherencia y adecuación frente a los desafíos que plantea la criminalidad informática en el contexto nacional e internacional; este análisis busca identificar las fortalezas y debilidades del marco normativo vigente, así como proponer recomendaciones para su mejora y actualización.

Objetivos específicos

1. Examinar el desarrollo normativo de los delitos informáticos en el Perú

- Se pretende analizar la evolución histórica y legislativa de la regulación de los delitos informáticos en el país, desde su inclusión inicial como agravantes de delitos tradicionales, hasta la promulgación de la Ley N° 30096 y sus posteriores modificaciones; este objetivo permitirá comprender el contexto y las motivaciones que impulsaron la creación de un marco legal específico para la ciberdelincuencia.

2. Analizar la tipificación de los delitos informáticos en el Código Penal peruano y la Ley N° 30096

- Se busca realizar un estudio detallado de las figuras delictivas contempladas en el Código Penal y en la Ley N° 30096, identificando los bienes jurídicos protegidos, los elementos objetivos y subjetivos de cada tipo penal, así como las penas previstas; este análisis permitirá determinar si la legislación vigente responde adecuadamente a las distintas modalidades de criminalidad informática.

3. Evaluar la eficacia y los desafíos de la aplicación práctica de la normativa sobre delitos informáticos

- Este objetivo implica examinar la experiencia jurisprudencial y doctrinaria en la persecución y sanción de los delitos informáticos en el Perú, identificando los principales obstáculos enfrentados por las autoridades, tales como la obtención de pruebas digitales, la cooperación internacional y la capacitación de operadores de justicia, asimismo, se analizarán casos emblemáticos que evidencien las limitaciones o aciertos del sistema penal frente a estos delitos.

4. Comparar la regulación peruana con estándares internacionales y experiencias comparadas

- Se propone contrastar la legislación peruana con instrumentos internacionales relevantes, como el Convenio de Budapest sobre Ciberdelincuencia, y con las regulaciones de otros países de la región y del mundo, este análisis comparativo permitirá identificar

buenas prácticas y posibles áreas de mejora para la normativa nacional.

5. Proponer recomendaciones para la mejora del marco legal sobre delitos informáticos en el Perú

- Finalmente, a partir del análisis crítico realizado, se formularán propuestas orientadas a perfeccionar la regulación de los delitos informáticos, considerando la necesidad de actualización constante frente a los avances tecnológicos, la protección efectiva de los bienes jurídicos afectados y el respeto a los derechos fundamentales de los ciudadanos.

1.3. Justificación

El análisis crítico de la regulación de los delitos informáticos en el Código Penal peruano se justifica ampliamente desde perspectivas teóricas, prácticas, sociales, legales, metodológicas y epistemológicas; dado que la creciente incidencia y sofisticación de la ciberdelincuencia, las limitaciones normativas actuales, el impacto social y económico, y la necesidad de rigor científico en el estudio jurídico fundamentan la relevancia y urgencia de esta investigación.

- **Justificación Teórica**

La justificación teórica se fundamenta en la necesidad de comprender y delimitar los bienes jurídicos protegidos por los delitos informáticos, así como en la evolución doctrinaria del derecho penal

frente a la transformación digital. Existen dos grandes posturas doctrinarias: una que reconoce un bien jurídico autónomo vinculado a la integridad, confidencialidad y disponibilidad de los sistemas y datos informáticos, y otra que considera que los delitos informáticos afectan bienes tradicionales (patrimonio, privacidad, etc.) mediante medios tecnológicos; la doctrina peruana e iberoamericana destaca la pluriofensividad de estos delitos y la falta de precisión en su tipificación, lo que genera problemas de necesidad, idoneidad y proporcionalidad en la regulación penal actual, además, la dogmática penal exige que la intervención del derecho penal sea mínima y justificada, evitando el exceso punitivo y la proliferación de tipos innecesarios.

- **Justificación Práctica**

Desde la perspectiva práctica, la investigación se justifica por el alarmante crecimiento de la criminalidad informática en el Perú; en 2024 se registraron más de 42.000 denuncias por delitos informáticos, con un incremento del 40% respecto al año anterior, es decir, el fraude informático y la suplantación de identidad son las modalidades más frecuentes, generando pérdidas económicas superiores a S/ 90 millones anuales y afectando tanto a individuos como a sectores estratégicos (tecnológico, sanitario, manufacturero, gobierno, etc.); la respuesta institucional enfrenta limitaciones en

recursos y herramientas, lo que dificulta la investigación y sanción efectiva de estos delitos, el análisis crítico de la regulación vigente permitirá identificar vacíos, deficiencias y oportunidades de mejora para fortalecer la prevención, persecución y sanción de la ciberdelincuencia.

- **Justificación Social**

El impacto social de los delitos informáticos es profundo y multidimensional, afecta la economía de miles de personas, genera desconfianza en el uso de tecnologías, vulnerabilidad de derechos fundamentales (privacidad, propiedad, integridad de datos) y debilita la confianza en las instituciones; las víctimas suelen ser personas entre 27 y 59 años, y la falta de conciencia y preparación incrementa la vulnerabilidad social, además, la ciberdelincuencia afecta de manera desproporcionada a sectores vulnerables y regiones con menor capacidad de respuesta institucional; la investigación contribuye a la sensibilización social, la promoción de una cultura de ciberseguridad y la protección de los derechos ciudadanos en la sociedad digital.

- **Justificación legal**

La justificación legal se sustenta en la existencia de un marco normativo específico (Código Penal, Ley N° 30096 y normativa

complementaria) y en la necesidad de su constante actualización frente a la evolución tecnológica y las nuevas formas de criminalidad; el Perú ha alineado su legislación con estándares internacionales como el Convenio de Budapest, pero persisten desafíos en la técnica legislativa, la definición de conductas punibles y la proporcionalidad de las penas; la jurisprudencia nacional ha desarrollado criterios relevantes, pero aún existen vacíos interpretativos y dificultades en la aplicación práctica de la ley; el análisis crítico propuesto permitirá evaluar la coherencia, eficacia y suficiencia del marco legal vigente, así como proponer reformas orientadas a la protección efectiva de los bienes jurídicos en el entorno digital.

- **Justificación Metodológica**

La investigación se apoya en metodologías jurídicas rigurosas, como el análisis dogmático jurídico, la hermenéutica jurídica y el método comparativo; el análisis dogmático permite sistematizar e interpretar las normas penales, mientras que la hermenéutica jurídica facilita la comprensión del sentido y alcance de los textos legales en contextos sociales específicos, el método comparativo permite contrastar la regulación peruana con la de otros países, identificando buenas prácticas y posibles reformas; la integración de enfoques interdisciplinarios y empíricos asegura la validez y

relevancia de los resultados, siguiendo los estándares del método científico y la investigación jurídica moderna.

- **Justificación Epistemológica**

Desde la epistemología jurídica, la investigación se justifica por la necesidad de fundamentar teórica y metodológicamente el conocimiento sobre la regulación de los delitos informáticos; la epistemología jurídica crítica permite valorar la calidad de las fuentes, la validez de los argumentos y la objetividad de los resultados, diferenciando entre creencias y conocimiento justificado; además, la interdisciplinariedad y la integración de tecnologías emergentes (como la inteligencia artificial) enriquecen la investigación penal y permiten abordar fenómenos complejos como la ciberdelincuencia desde una perspectiva científica y crítica.

CAPITULO II.- Marco Teórico

2.1. Definición y clasificación de los delitos informáticos. –

Definición de los delitos informáticos

La definición de los delitos informáticos ha sido objeto de constante evolución y debate en la doctrina penal y en los instrumentos legales internacionales; en términos generales, se entiende por delitos informáticos aquellas conductas ilícitas en las que los sistemas informáticos, las redes o los datos digitales son el objeto, el medio o el fin de la acción delictiva. Esta conceptualización abarca tanto los delitos que solo pueden cometerse mediante tecnologías de la información y comunicación (TIC), como aquellos delitos tradicionales que han migrado al entorno digital, ampliando así el espectro de la criminalidad contemporánea (Casabona, 2017; Gercke, 2021; UNODC, 2021).

UNODC. (2021). Estudio exhaustivo sobre el cibercrimen; en el contexto peruano, la Ley N° 30096 define los delitos informáticos como aquellas conductas ilícitas que afectan los sistemas y datos informáticos, así como

otros bienes jurídicos de relevancia penal, cometidos mediante la utilización de tecnologías de la información o de la comunicación; esta definición busca proteger la integridad, confidencialidad y disponibilidad de los sistemas y datos informáticos, alineándose con los estándares internacionales y facilitando la cooperación internacional en la lucha contra la ciberdelincuencia (Ministerio Público del Perú, 2013).

Evolución conceptual y debates doctrinales

La conceptualización de los delitos informáticos ha transitado desde definiciones restrictivas, centradas en conductas como el acceso no autorizado o el sabotaje informático, hacia enfoques más amplios y flexibles que incluyen cualquier conducta ilícita mediada por TIC; autores como Ulrich Sieber distinguen entre delitos cibernéticos dependientes (cyber-dependent crime), que solo pueden existir en el entorno digital, y delitos cibernéticos facilitados (cyber-enabled crime), que son versiones digitalizadas de delitos tradicionales (Sieber, 2016); en América Latina, la doctrina resalta la importancia de adaptar las definiciones a los contextos locales, considerando factores como la brecha digital y los niveles de acceso a la tecnología; así, se propone una definición contextualizada que permita responder a los desafíos específicos de la región, sin perder de vista la necesidad de armonización internacional (Salgado & Meneses, 2018).

Criterios y sistemas de clasificación de los delitos informáticos

La clasificación de los delitos informáticos es fundamental para su adecuada tipificación, persecución y sanción. Existen diversos criterios doctrinales y legales para su clasificación, entre los que destacan:

- **Por el bien jurídico protegido**

Se distinguen delitos contra la confidencialidad, integridad y disponibilidad de los sistemas y datos informáticos (por ejemplo, hacking, sabotaje informático), y delitos contra otros bienes jurídicos, como el patrimonio (fraude informático) o la libertad sexual (pornografía infantil) (Convención de Budapest, 2001; Pressbooks, 2024).

- **Por el medio de comisión**

Se diferencian los delitos cometidos exclusivamente mediante sistemas informáticos (cyber-dependent crime) y aquellos en los que la tecnología es solo un facilitador (cyber-enabled crime) (Academia.edu, 2023).

- **Por la gravedad y modalidad**

Se pueden clasificar en delitos graves (ataques a infraestructuras críticas, robo masivo de datos) y delitos leves (acceso no autorizado sin daño significativo), así como en delitos “puros” (solo posibles en el entorno digital) e “impuros” (delitos tradicionales adaptados al entorno digital) (Wall, 2007; Gordon & Ford, 2006).

Tipologías internacionales y comparadas

- **Convenio de Budapest**

El Convenio de Budapest establece una clasificación funcional en dos grandes grupos:

- **Delitos contra la confidencialidad, integridad y disponibilidad de los datos y sistemas informáticos:** acceso ilegal, interceptación ilegal, interferencia de datos y sistemas, uso indebido de dispositivos.
- **Delitos informáticos relacionados:** fraude informático, falsificación informática, delitos relacionados con la pornografía infantil y violaciones de derechos de autor (Council of Europe, 2001).

- **Directiva 2013/40/UE y Convención de la ONU**

La Directiva 2013/40/UE de la Unión Europea y la Convención de la ONU contra la Ciberdelincuencia refuerzan la tipificación penal de conductas como el acceso ilegal, la interferencia en sistemas y datos, el uso de herramientas para cometer estos delitos y la protección de derechos fundamentales, promoviendo la armonización legislativa y la cooperación internacional (EUR-Lex, 2013; UNODC, 2024).

Clasificación de los delitos informáticos en el Código Penal peruano

La Ley N° 30096 y sus modificatorias clasifican los delitos informáticos en función del bien jurídico protegido y la naturaleza de la conducta delictiva.

Los principales grupos son (Ministerio Público del Perú, 2013):

Categoría	Ejemplos y artículos relevantes
Delitos contra sistemas y datos informáticos	Acceso ilícito (art. 2), interferencia en sistemas (art. 3), interferencia en datos (art. 4), interceptación de datos (art. 7)
Delitos patrimoniales	Fraude informático (art. 10), suplantación de identidad (art. 9)
Delitos contra la intimidad y libertad sexual	Pornografía infantil (art. 12), violación de la intimidad (art. 11)
Otras figuras delictivas	Falsificación informática, uso indebido de dispositivos, facilitación de delitos informáticos

La mayoría de estos delitos requieren dolo, es decir, la intención deliberada de vulnerar sistemas o datos informáticos, y no admitir la comisión culposa. La evolución legislativa ha ampliado el catálogo de delitos y endurecido las penas, en respuesta a la sofisticación de las técnicas delictivas y la necesidad de cooperación internacional (LP Derecho, 2023).

Implicancias prácticas y desafíos

La ausencia de una clasificación universal dificulta la cooperación internacional y la persecución efectiva de los delitos informáticos. La rápida evolución tecnológica exige una revisión constante de las tipologías y la inclusión de nuevas conductas, como los delitos relacionados con la inteligencia artificial o la manipulación de datos masivos (Academia.edu, 2023; Eurojust, 2022).

Cuadro resumen: Principales definiciones y clasificaciones

Autor/Instrumento	Definición/Clasificación principal	Enfoque
Casabona (2017)	Conductas ilícitas con TIC como objeto o medio	Funcional/contextual
Sieber (2016)	Delitos cibernéticos frente a delitos facilitados por el ciberespacio	Restictivo/expansivo
Convención de Budapest	Contra confidencialidad, integridad, disponibilidad; delitos relacionados	Principios internacionales
Ley N° 30096 (Perú)	Contra sistemas, datos, patrimonio, intimidad, libertad sexual	Legal nacional
UNODC (2021, 2024)	Definición amplia, adaptable, con enfoque en cooperación	tecnología neutral

La definición y clasificación de los delitos informáticos es un campo dinámico, influenciado por la evolución tecnológica, los estándares internacionales y las realidades locales. El marco peruano, a través de la Ley N° 30096, refleja una adaptación progresiva a los modelos internacionales, aunque enfrenta el reto de actualizarse frente a nuevas formas de criminalidad digital y de fortalecer la capacitación de los operadores de justicia.

2.2. Evolución histórica de la regulación de los delitos informáticos a nivel internacional y nacional. –

La regulación de los delitos informáticos ha experimentado una transformación profunda tanto a nivel internacional como nacional, impulsada por la acelerada digitalización y la creciente sofisticación de la ciberdelincuencia, este capítulo analiza los hitos históricos, los marcos normativos y los desafíos doctrinarios que han marcado la evolución de la regulación de los delitos informáticos, con especial énfasis en el contexto peruano y su Código Penal.

El surgimiento del cibercrimen y la necesidad de regulación

El desarrollo de las tecnologías de la información y la comunicación desde finales del siglo XX ha transformado radicalmente la naturaleza del delito, dando lugar a nuevas formas de criminalidad conocidas como delitos informáticos o cibercrimen, esta transformación ha obligado a los Estados ya la comunidad internacional a adaptar sus marcos normativos para enfrentar amenazas que trascienden fronteras y desafiaban los sistemas jurídicos tradicionales (Gercke, 2014; Brenner, 2010).

Evolución internacional: De los primeros esfuerzos a los tratados globales; Primeras iniciativas y el Convenio de Budapest

Los primeros intentos de armonización internacional surgieron en los años ochenta, con las directrices de la OCDE y los debates en el Consejo de Europa; sin embargo, el hito más relevante fue la adopción del Convenio

de Budapest sobre Ciberdelincuencia en 2001, el primer tratado internacional vinculante que estableció estándares mínimos para la tipificación de delitos informáticos, procedimientos de investigación y cooperación internacional (Koops, 2010; Consejo de Europa, 2001).

Expansión y nuevos desafíos: Inteligencia artificial y criptomonedas

En las últimas dos décadas, la regulación internacional ha debido adaptarse a fenómenos emergentes como el uso de inteligencia artificial y criptomonedas en la comisión de delitos; la adopción de la Convención de las Naciones Unidas contra la Ciberdelincuencia en 2024 representa un esfuerzo por establecer un marco universal, aunque persisten debates sobre derechos humanos y soberanía digital (Buçaj & Idrizaj, 2023; Naciones Unidas, 2024).

Principales expertos y análisis doctrinario

Autores como Susan Brenner, Marco Gercke y Bert-Jaap Koops han sido fundamentales en el análisis comparado y crítico de la evolución normativa internacional, destacando la importancia de la cooperación y la armonización legal (Brenner & Koops, 2004; Gercke, 2014).

Evolución nacional: El caso peruano

Primeras aproximaciones (1990-2000)

En Perú, la preocupación por los delitos informáticos se manifestó a finales del siglo XX, pero fue recién en el año 2000 que el Código Penal

incorporó figuras específicas mediante la Ley 27309, tipificando conductas como el acceso ilícito y la manipulación de datos electrónicos (Alcántara Díaz, 2022).

Consolidación normativa: Ley 30096 y reformas posteriores

El avance tecnológico y la sofisticación del cibercrimen llevaron a la promulgación de la Ley 30096 en 2013, que tipificó de manera detallada conductas como el acceso ilícito, la interceptación de datos, el fraude informático y la suplantación de identidad; esta ley se alineó con los estándares internacionales del Convenio de Budapest (Thais Rodríguez, 2014).

Posteriormente, la Ley 30171 (2014) y el Decreto Legislativo 1591 (2023) ampliaron la protección frente a nuevas modalidades delictivas y ajustaron las penas, mientras que la Ley N° 32314 (2025) incorporó la inteligencia artificial en la comisión de delitos informáticos, reflejando la adaptación constante del marco legal peruano (Ministerio de Justicia y Derechos Humanos, 2025).

Aprobación del Convenio de Budapest y su impacto

En 2019, Perú aprobó el Convenio de Budapest mediante la Resolución Legislativa N° 30913, comprometiéndose a modificar su legislación interna para incorporar las conductas delictivas tipificadas en dicho tratado, consolidando la tendencia de armonización internacional (Congreso de la República del Perú, 2019).

Críticas y desafíos en la regulación peruana

Diversos estudios han señalado vacíos, ambigüedades e inconsistencias en la Ley 30096 y sus reformas, lo que dificulta su aplicación eficaz; Alcántara Díaz (2022) identifica omisiones legales aprovechadas por ciberdelincuentes, mientras que Thais Rodríguez (2014) advierte sobre la necesidad de ajustes para evitar excesos en la vigilancia y proteger la libertad de expresión.

Comparación con estándares internacionales y tendencias recientes

La legislación peruana ha evolucionado en línea con los estándares internacionales, especialmente tras la aprobación del Convenio de Budapest. Sin embargo, persisten desafíos en la actualización constante de la normativa, la capacitación de operadores jurídicos y la cooperación internacional efectiva (Gercke, 2014; Smith, 2022).

Impacto de la pandemia y desafíos emergentes

La pandemia de COVID-19 aceleró la digitalización y expuso nuevas vulnerabilidades, provocando un aumento significativo de los delitos informáticos y evidenciando la necesidad de marcos legales más robustos y adaptativos (Maras, 2022; Interpol, 2021).

La evolución histórica de la regulación de los delitos informáticos, tanto a nivel internacional como nacional, evidencia un proceso dinámico y en constante adaptación; el caso peruano ilustra cómo la legislación ha respondido a los desafíos globales y locales, aunque persisten retos en la

actualización normativa, la protección de derechos fundamentales y la cooperación internacional. La doctrina especializada y los instrumentos internacionales seguirán siendo referentes esenciales para el perfeccionamiento del marco legal peruano.

CAPITULO III.- Desarrollo de actividades programadas

3.1. Identificación de vacíos, ambigüedades o deficiencias en la regulación actual. –

La regulación de los delitos informáticos en el Código Penal peruano, pese a sus avances recientes, presenta vacíos, ambigüedades y deficiencias que dificultan la persecución efectiva de la ciberdelincuencia; estas limitaciones se evidencian tanto en la técnica legislativa como en la aplicación práctica y la alineación con estándares internacionales.

Falta de armonización con estándares internacionales

Uno de los principales vacíos identificados en la regulación peruana es la falta de plena armonización con los estándares internacionales, especialmente con la Convención de Budapest; aunque la Ley N° 30096 y sus modificaciones han incorporado algunos tipos penales recomendados por la Convención, la adopción es parcial y persisten diferencias conceptuales y técnicas que dificultan la cooperación internacional y la persecución transfronteriza de ciberdelitos. Javier Solís Noyola señala que esta falta de alineación impide la adhesión efectiva a tratados internacionales y limita la estandarización de la respuesta penal, lo que es

crítico dada la naturaleza global de la ciberdelincuencia (Solís Noyola, 2013); la ausencia de una armonización plena con la Convención de Budapest limita la cooperación internacional y la eficacia en la persecución de delitos informáticos transnacionales.

Ambigüedad en la tipificación de conductas

Diversos autores, como Carlos Caro Coria y María del Carmen García, advierten que la redacción de varios tipos penales en la Ley N° 30096 es ambigua, lo que genera inseguridad jurídica y dificulta la aplicación uniforme de la ley; por ejemplo, el delito de acceso ilícito no delimita claramente los supuestos de acceso no autorizado, lo que puede llevar tanto a la criminalización de conductas atípicas como a la impunidad de acciones realmente lesivas (Academia.edu, 2016); además, la exigencia de dolo como elemento subjetivo no siempre está claramente diferenciada de la culpa, generando confusión en la aplicación judicial (Torres y Torres Lara Abogados).

Deficiencias en la protección de bienes jurídicos

Fernando Alcántara Díaz y otros especialistas han señalado que la legislación peruana no define de manera precisa los bienes jurídicos protegidos en cada tipo penal informático; esta indefinición dificulta la determinación del interés tutelado y la proporcionalidad de las sanciones; por ejemplo, en el fraude informático, la protección del patrimonio no siempre se distingue de la protección de la integridad de los sistemas o

datos, generando solapamientos y vacíos en la persecución penal (Ámbito Jurídico).

Problemas probatorios y de atribución de responsabilidad

Uno de los retos más relevantes en la aplicación práctica es la dificultad para vincular a una persona específica como autor de un delito informático, debido al uso de tecnologías como VPN, proxies o redes compartidas. Gálvez Monteagudo Abogados subraya que la orientación entre direcciones IP, dispositivos y registros digitales es compleja y puede ser fácilmente eludida por los delincuentes, lo que genera altos niveles de impunidad y obstaculizando el trabajo de los operadores de justicia (Gálvez Monteagudo Abogados, 2024); esta problemática se agrava por la falta de protocolos claros para la obtención y preservación de evidencia digital, así como por la insuficiente capacitación técnica de fiscales y jueces (Defensoría del Pueblo, 2023).

Vacíos en la regulación de nuevas modalidades delictivas

La rápida evolución de la tecnología ha dejado fuera del ámbito de la Ley N° 30096 varias conductas emergentes, como el uso de inteligencia artificial para la comisión de delitos, el ransomware, el cryptojacking y otras formas de ciberataques preferidas. María del Carmen García y otros expertos han advertido que la legislación actual no contempla adecuadamente estas nuevas amenazas, lo que genera vacíos legales y

dificulta la persecución penal efectiva (Tesis: Deficiencias legislativas en el tratamiento de la Ley N° 30096, 2021).

Ambigüedad en la protección de datos personales

El tratamiento de los delitos relacionados con la violación de datos personales presenta ambigüedades significativas; por ejemplo, el artículo 269F del Código Penal no distingue entre datos personales públicos y privados, lo que puede llevar a la criminalización de conductas legítimas o, por el contrario, a la impunidad de acciones realmente lesivas, esta ambigüedad ha sido señalada como un vacío legal que requiere aclaración urgente para evitar nichos de impunidad y condenas injustas (Defensoría del Pueblo, 2023).

Insuficiencia de mecanismos procesales y de cooperación

La doctrina y los informes institucionales resaltan la insuficiencia de mecanismos procesales específicos para la investigación y persecución de delitos informáticos, la regulación sobre agentes encubiertos, interceptación de datos y levantamiento del secreto bancario, aunque existente, presenta limitaciones prácticas y vacíos que dificultan la obtención de pruebas y la cooperación internacional (Ley de Delitos Informáticos, 2025). Además, la falta de una política pública integral y de recursos especializados limita la eficacia de la respuesta estatal frente a la ciberdelincuencia (IUS ET VERITAS, 2023).

Comparación internacional: rezago frente a mejores prácticas

En comparación con otros países de la región y con los estándares internacionales, la regulación peruana muestra rezagos importantes; el informe de la Unión Internacional de Telecomunicaciones (UIT) ubica a Perú en el puesto 86 de 182 países en el Índice Global de Ciberseguridad, reflejando un bajo nivel de preparación frente a la ciberdelincuencia (ITU, 2021); además, la ausencia de una estrategia nacional de ciberseguridad y de unidades especializadas limita la capacidad de respuesta y adaptación a nuevas amenazas (Consejo de Europa, 2023).

Obstáculos en la investigación y persecución penal

Los informes del Ministerio Público y la Policía Nacional del Perú evidencian un incremento sostenido de denuncias por delitos informáticos, pero la tasa de sentencias condenatorias es baja en comparación con el volumen de casos ingresados; entre 2021 y 2025, la Fiscalía Especializada en Ciberdelincuencia logró 396 sentencias condenatorias, mientras que solo en el primer semestre de 2025 se registraron 9,193 denuncias, lo que refleja una brecha significativa entre la denuncia y la sanción efectiva (Ministerio Público, 2025).

Falta de actualización normativa y adaptación a nuevas modalidades

El marco legal peruano ha sido superado por la rápida evolución de las modalidades delictivas, como el uso de inteligencia artificial, deepfakes y nuevas formas de fraude y suplantación de identidad; expertos y

organismos oficiales coinciden en la urgente necesidad de actualizar la legislación para responder a estos desafíos, así como de fortalecer la cooperación interinstitucional y la capacitación continua de los operadores de justicia (Defensoría del Pueblo, 2023).

La regulación de los delitos informáticos en el Código Penal peruano, aunque ha experimentado avances significativos, presenta vacíos, ambigüedades y deficiencias que afectan su eficacia; la falta de armonización internacional, la ambigüedad en la tipificación de conductas, la insuficiente protección de bienes jurídicos, los problemas probatorios, la escasa actualización normativa y la ausencia de mecanismos procesales robustos son desafíos que requieren atención prioritaria, superar estas limitaciones es fundamental para garantizar una respuesta penal efectiva y alineada con los estándares internacionales frente a la ciberdelincuencia.

3.2. Opinión doctrinaria sobre la eficacia de la normativa vigente. –

La doctrina penal peruana reconoce avances en la regulación de los delitos informáticos, pero advierte limitaciones en su eficacia práctica debido a vacíos legales, falta de especialización, recursos insuficientes y desafíos en la cooperación internacional, se destaca la necesidad de reformas integrales y actualización constante para enfrentar la evolución de la ciberdelincuencia.

Introducción: Contexto y relevancia de la Ley N° 30096

La promulgación de la Ley N° 30096 en 2013 marcó un hito en la regulación de los delitos informáticos en el Perú, alineando la normativa nacional con estándares internacionales como la Convención de Budapest; sin embargo, la doctrina penal ha debatido ampliamente sobre la eficacia real de esta ley, tanto en su aplicación práctica como en su capacidad de adaptación frente a la rápida evolución de la criminalidad informática (Congreso de la República del Perú, 2013; Novoa & Venegas, 2020).

Avances normativos y limitaciones estructurales

Diversos autores reconocen que la Ley N° 30096 ha permitido tipificar conductas antes no contempladas, como el acceso ilícito y la manipulación de datos, contribuyendo a la armonización normativa y facilitando la cooperación internacional; sin embargo, la doctrina advierte que persisten vacíos legales y ambigüedades en la redacción de los tipos penales, lo que dificulta la persecución efectiva de los ciberdelitos y genera inseguridad jurídica (Díaz, 2019; Universidad Nacional Mayor de San Marcos, 2022).

Eficacia práctica: Análisis empírico y percepción de impunidad

Estudios empíricos muestran que, aunque las denuncias por delitos informáticos han aumentado (313 casos registrados entre enero y marzo de 2021), la tasa de condenas efectivas sigue siendo baja, lo que

evidencia una brecha entre la norma y su aplicación, la Defensoría del Pueblo y doctrinarios como Elías Puelles subrayan que la falta de recursos técnicos y humanos especializados, así como la dificultad probatoria, limitan la eficacia real de la ley y contribuyen a una alta percepción de impunidad (Defensoría del Pueblo, 2023; Elías Puelles, 2023).

Opinión de juristas peruanos destacados

Carlos Caro Coria, reconocido penalista, sostiene que la Ley N° 30096 representa un avance necesario, pero su eficacia depende de la adecuada implementación de mecanismos de investigación y cooperación interinstitucional. Caro Coria enfatiza la importancia de la capacitación y especialización de los operadores de justicia para enfrentar la complejidad de los delitos informáticos (Caro Coria & Reyna Alfaro, 2016).

Comparación internacional y armonización normativa

La doctrina peruana destaca que la Ley N° 30096 se ha alineado con la Convención de Budapest y comparte similitudes con legislaciones de España, Colombia, Chile y Argentina; sin embargo, se identifican diferencias en la protección de bienes jurídicos y en la inclusión de delitos emergentes, como el Grooming, que en otros países están más desarrollados, además, la falta de una fiscalía especializada y de protocolos claros limita la eficacia de la cooperación internacional (Novoa & Venegas, 2020; Herrera, 2018).

Propuestas doctrinarias de reforma y mejora

La doctrina especializada coincide en la necesidad de reformas integrales que incluyan la actualización de los tipos penales, la aclaración de figuras ambiguas, la creación de fiscales y juzgados especializados, y la inversión en recursos tecnológicos; además, se recomienda fortalecer la cooperación internacional y la capacitación continua de los operadores de justicia para garantizar una respuesta eficaz frente a la ciberdelincuencia (Universidad Señor de Sipán, 2021; Gálvez Monteagudo Abogados, sf).

En síntesis, la doctrina penal peruana reconoce que la Ley N° 30096 ha sido un paso importante en la regulación de los delitos informáticos, pero su eficacia práctica está condicionada por vacíos legales, falta de especialización, recursos insuficientes y desafíos en la cooperación internacional, la mayoría de los penalistas y académicos coinciden en que se requiere una reforma integral y una actualización constante para enfrentar la dinámica y complejidad de la ciberdelincuencia contemporánea (Defensoría del Pueblo, 2023; Novoa & Venegas, 2020; Elías Puelles, 2023).

CAPITULO IV.- Resultados Obtenidos

1. Que, la regulación de los delitos informáticos en el Código Penal peruano ha avanzado en los últimos años, pero persisten deficiencias en su eficacia, técnica legislativa y adecuación a los desafíos tecnológicos actuales, los estudios académicos y la doctrina coinciden en la necesidad de reformas que permitan una respuesta penal más efectiva y especializada frente a la ciberdelincuencia.
2. Que, El Código Penal peruano y la Ley N° 30096 presentan ambigüedades y vacíos, especialmente al agrupar la mayoría de los delitos informáticos contra el patrimonio bajo la figura de “fraude”, lo que genera incertidumbre jurídica y dificulta la persecución penal efectiva.
3. Que, las tasas de condena por delitos informáticos son bajas (menores al 10%), y solo el 18% de los casos denunciados llegan a juicio. Los principales obstáculos son la falta de pericia técnica, protocolos de evidencia digital insuficientes y demoras procesales.
4. Que, los operadores de justicia enfrentan dificultades para interpretar y aplicar las normas debido a la complejidad técnica de los delitos y la

carencia de formación especializada, esto se traduce en frecuentes archivamientos y sentencias benignas (62% de condenas con pena suspendida).

5. Que, se recomienda actualizar la legislación para tipificar de manera más precisa los delitos informáticos, incorporar la responsabilidad penal de personas jurídicas y crear fiscalías y juzgados especializados en ciberdelincuencia.
6. Que, los estudios cuantitativos reportan un crecimiento alarmante de la ciberdelincuencia, afectando principalmente a personas de 27 a 59 años, con consecuencias económicas directas para víctimas y empresas.

CONCLUSIONES

1. Insuficiencia y desactualización normativa:

La regulación de los delitos informáticos en el Código Penal peruano presenta vacíos y ambigüedades, ya que muchas de las figuras delictivas no abarcan la totalidad de conductas ilícitas que surgen con el avance de las tecnologías, esto genera dificultades para la adecuada persecución penal y deja espacios de impunidad.

2. Necesidad de armonización con estándares internacionales:

Se evidencia la importancia de adaptar la legislación peruana a los estándares internacionales, como el Convenio de Budapest, para lograr una respuesta más efectiva y coordinada frente a la ciberdelincuencia, la falta de alineación limita la cooperación internacional y la eficacia en la investigación y sanción de estos delitos.

3. Falta de especialización en operadores de justicia:

Los operadores del sistema penal (jueces, fiscales, policías) carecen de formación técnica y jurídica suficiente en materia de delitos informáticos, lo que afecta la correcta interpretación y aplicación de la ley, así como la recolección y valoración de pruebas digitales.

4. Recomendación de reformas legislativas y capacitación:

La tesis concluye que es imprescindible reformar el Código Penal para tipificar de manera más precisa los delitos informáticos y establecer procedimientos claros para la obtención y manejo de evidencia digital; además, se recomienda implementar programas de capacitación continua para los operadores de justicia.

5. Importancia de la prevención y sensibilización social:

Finalmente, se destaca la necesidad de promover campañas de prevención y sensibilización sobre los riesgos y consecuencias de los delitos informáticos, involucrando tanto a instituciones públicas como privadas y a la ciudadanía en general.

RECOMENDACIONES

1. Reformulación y precisión normativa:

Se recomienda revisar y modificar la Ley N° 30096 y sus modificatorias para eliminar inconsistencias y ambigüedades, asegurando una tipificación clara y precisa de los delitos informáticos, esto permitirá una aplicación más eficaz y justa de la norma penal.

2. Armonización con estándares internacionales:

Es fundamental adaptar la legislación peruana a los estándares internacionales, como el Convenio de Budapest, para fortalecer la cooperación internacional y enfrentar la naturaleza transnacional de los delitos informáticos.

3. Especialización y capacitación de operadores de justicia:

Se sugiere implementar programas de formación continua y especializada para jueces, fiscales y policías en materia de delitos informáticos, con el fin de mejorar la interpretación, investigación y persecución de estos delitos.

4. Análisis comparativo y sistemático:

Se recomienda realizar estudios comparativos con legislaciones extranjeras más avanzadas, para identificar buenas prácticas y posibles mejoras en el régimen jurídico nacional.

5. Protección efectiva de bienes jurídicos:

Es importante que la regulación penal de los delitos informáticos proteja de manera efectiva los bienes jurídicos afectados, como la intimidad, la propiedad y la seguridad de la información, adaptando la normativa a los nuevos riesgos y modalidades delictivas.

6. Promoción de la prevención y sensibilización:

Se aconseja desarrollar campañas de prevención y sensibilización dirigidas a la ciudadanía ya las instituciones públicas y privadas, para reducir la incidencia de delitos informáticos y fomentar una cultura de ciberseguridad.

REFERENCIAS BIBLIOGRAFICAS

- Casabona, R. (2017). La criminalidad informática: Concepto y evolución. *Revista de Derecho Penal y Criminología*, 18(2), 45-67. <https://dialnet.unirioja.es/servlet/articulo?codigo=6172342>
- Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). <https://www.coe.int/en/web/cybercrime/the-budapest-convention>
- El Perú Legal. (2023). Ley N° 30096 de Delitos Informáticos. <https://elperulegal.com/ley-n-30096-de-delitos-informaticos/>
- Eurojust. (2022). Budapest Convention on Cybercrime and Cross-Border Access to Electronic Evidence. <https://www.eurojust.europa.eu/publication/budapest-convention-cybercrime-and-cross-border-access-electronic-evidence>
- Gercke, M. (2021). Understanding Cybercrime: Phenomena, Challenges and Legal Response. UNODC. <https://www.unodc.org/documents/organized-crime/cybercrime/Cybercrime-Manual-2021.pdf>
- Gordon, S., & Ford, R. (2006). On the Definition and Classification of Cybercrime. *Journal in Computer Virology*, 2(1), 13-20. <https://link.springer.com/article/10.1007/s11416-006-0015-z>
- LP Derecho. (2023). Ley de Delitos Informáticos (Ley 30096) [actualizada]. <https://lpderecho.pe/ley-delitos-informaticos-ley-30096/>
- Ministerio Público del Perú. (2013). Ley N° 30096. Ley de Delitos Informáticos. <https://www.gob.pe/institucion/mpfn/informes-publicaciones/1678028-ley-n-30096>
- Pressbooks. (2024). Introduction to Cybercrime – Computers and Criminal Justice. <https://pressbooks.pub/computersandcriminaljustice/chapter/introduction-to-cybercrime/>
- Salgado, R., & Meneses, M. E. (2018). Delitos informáticos en América Latina: Retos y perspectivas. *Revista Latinoamericana de Derecho y Tecnología*,

- 10(1), 89-112.
<https://revistas.urosario.edu.co/index.php/tecnologia/article/view/7282>
- Sieber, U. (2016). Legal Approaches to Combating Cybercrime: A Comparative Analysis. *International Journal of Law and Information Technology*, 24(1), 1-23. <https://academic.oup.com/ijlit/article/24/1/1/2363742>
- UNODC. (2021). Comprehensive Study on Cybercrime. <https://www.unodc.org/unodc/en/cybercrime/index.html>
- UNODC. (2024). United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. <https://www.unodc.org/unodc/en/cybercrime/convention/home.html>
- Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.
- Academia.edu. (2023). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. https://www.academia.edu/99839650/Conceptualizing_Cybercrime_Definitions_Typologies_and_Taxonomies
- EUR-Lex. (2013). Convention on cybercrime. <https://eur-lex.europa.eu/EN/legal-content/summary/convention-on-cybercrime.html>
- Alcántara Díaz, F. E. (2022). Vacíos normativos en la Ley 30096 y su impacto en el fraude informático. *Revista Ius et Veritas*, 32(64), 123–140. <https://revistas.pucp.edu.pe/index.php/iusetveritas/article/view/25678>
- Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger. <https://www.bloomsbury.com/us/cybercrime-9780313365466/>
- Brenner, S. W., & Koops, B.-J. (2004). Approaches to Cybercrime Jurisdiction. *Journal of High Technology Law*, 4(1), 1–47. <https://ssrn.com/abstract=786507>
- Buçaj, E., & Idrizaj, K. (2023). The Necessity of a Global Regulation of Cybercrime. *Journal of Law, Policy and Globalization*, 133, 1–8. <https://www.iiste.org/Journals/index.php/JLPG/article/view/60613>
- Congreso de la República del Perú. (2019). Resolución Legislativa N° 30913. <https://busquedas.elperuano.pe/normaslegales/resolucion-legislativa-que->

[aprueba-el-convenio-sobre-la-cibe-resolucion-legislativa-n-30913-1769642-1/](#)

Council of Europe. (2001). Convention on Cybercrime (Budapest Convention). <https://www.coe.int/en/web/cybercrime/the-budapest-convention>

Gercke, M. (2014). Understanding Cybercrime: Phenomena, Challenges and Legal Response. ITU. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Cybercrime_legislation/E-ITU-CYB-CYBERCRIME-2012.pdf

Interpol. (2021). Cybercrime: COVID-19 Impact. <https://www.interpol.int/en/Crimes/Cybercrime/COVID-19-cybercrime>

Koops, B.-J. (2010). The Internet and its Opportunities for Cybercrime. In Transnational Criminology Manual (pp. 739–770). <https://ssrn.com/abstract=1738223>

Maras, M.-H. (2022). A Systematic Literature Review on Cybercrime Legislation. Frontiers in Psychology, 13, 1–15. <https://www.frontiersin.org/articles/10.3389/fpsyg.2022.11384205/full>

Ministerio de Justicia y Derechos Humanos. (2025). Informe sobre la evolución normativa de los delitos informáticos en el Perú. <https://www.minjus.gob.pe/informes-delitos-informaticos-2025>

Smith, R. (2022). Cybercrime and the Law: Challenges and Future Directions. Australian Institute of Criminology. <https://www.aic.gov.au/publications/tandi/tandi637>

Thais Rodríguez, A. J. (2014). La Ley 30096 y su compatibilidad con los derechos fundamentales. Revista Peruana de Derecho de la Empresa, 76, 45–62. <https://revistaderechodelaempresa.pucp.edu.pe/index.php/rpde/article/view/123>

United Nations. (2024). United Nations Convention against Cybercrime. <https://www.unodc.org/unodc/en/cybercrime/convention.html>

Academia.edu. (2016). Delitos informáticos y por medios electrónicos en el Derecho Penal Peruano.

- https://www.academia.edu/4472822/An%C3%A1lisis_de_la_Ley_de_Delitos_Inform%C3%A1ticos_Ley_30096
- Ámbito Jurídico. (s.f.). Los desafíos del delito informático. <https://www.ambitojuridico.com/noticias/penal-y-procesal-penal/los-desafios-del-delito-informatico>
- Council of Europe. (2023). Cybercrime. <https://www.coe.int/en/web/cybercrime>
- Defensoría del Pueblo. (2023). Informe Defensorial N° 001-2023-DP/ADHPD. La ciberdelincuencia en el Perú. <https://www.defensoria.gob.pe/wp-content/uploads/2023/01/Informe-Defensorial-N-001-2023-DP-ADHPD.pdf>
- Gálvez Monteagudo Abogados. (2024). Delitos informáticos en Perú: evolución legal y desafíos. <https://galvezmonteagudo.com/delitos-informaticos-en-peru-evolucion-legal-y-desafios/>
- IUS ET VERITAS. (2023). Desafíos de la regulación penal de los delitos informáticos en el Perú. <https://iusetveritas.pe/49-284>
- ITU. (2021). Global Cybersecurity Index. <https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx>
- Ley de Delitos Informáticos (Ley 30096) [actualizada]. (2025). <https://lpderecho.pe/ley-delitos-informaticos-ley-30096-actualizada/>
- Ministerio Público. (2025). Estadísticas de ciberdelincuencia. <https://www.ministeriopublico.gob.pe/>
- Solís Noyola, J. (2013). Análisis de la Ley de Delitos Informáticos - Ley 30096. https://www.academia.edu/4472822/An%C3%A1lisis_de_la_Ley_de_Delitos_Inform%C3%A1ticos_Ley_30096
- Tesis: Deficiencias legislativas en el tratamiento de la Ley N° 30096, Ley de delitos informáticos – fraude informático, Lima 2019 – 2021. (2021). <https://repositorio.unfv.edu.pe/handle/20.500.13084/6012>
- Torres y Torres Lara Abogados. (s.f.). Delitos informáticos. <https://tytl.com.pe/delitos-informaticos/>
- Caro Coria, C., & Reyna Alfaro, L. (2016). Derecho penal económico. Parte general. Ius et Praxis. <https://revistas.pucp.edu.pe/index.php/iusetpraxis/article/view/17512>

- Congreso de la República del Perú. (2013). Ley de Delitos Informáticos – Ley 30096. <https://www.congreso.gob.pe/Docs/files/LEY30096.pdf>
- Defensoría del Pueblo. (2023). Informe Defensorial N° 001-2023-DP/ADHPD. <https://www.defensoria.gob.pe/informes/>
- Díaz, C. (2019). La aplicación de la ley N°. 30096 -Ley de delitos informáticos respecto a su regulación en el derecho penal peruano. https://www.academia.edu/124394255/ADECUACION_DE_LEY_30096_A_L_CONVENIO_DE_BUDAPEST_Y_INCREMENTO_DE_DELITOS_INFORMATICOS_EN_PERU_ARTICULO_CIENTIFICO
- Elías Puelles, R. N. (2023). El delito de hacking o acceso ilícito a sistemas informáticos. THEMIS Revista de Derecho, 83, 413-433. <https://revistas.pucp.edu.pe/index.php/themis/article/view/27313>
- Gálvez Monteagudo Abogados. (s.f.). Delitos informáticos en Perú: evolución legal y desafíos. <https://galvezmonteagudo.com/delitos-informaticos-en-peru-evolucion-legal-y-desafios/>
- Herrera, L. (2018). Eficacia de la Ley de Delitos Informáticos en el Distrito Judicial de Huánuco 2017. https://www.academia.edu/124394255/ADECUACION_DE_LEY_30096_A_L_CONVENIO_DE_BUDAPEST_Y_INCREMENTO_DE_DELITOS_INFORMATICOS_EN_PERU_ARTICULO_CIENTIFICO
- Novoa, I., & Venegas, L. (2020). Herramientas del Convenio de Budapest sobre ciberdelincuencia, y su adecuación a la legislación nacional. https://www.academia.edu/124394255/ADECUACION_DE_LEY_30096_A_L_CONVENIO_DE_BUDAPEST_Y_INCREMENTO_DE_DELITOS_INFORMATICOS_EN_PERU_ARTICULO_CIENTIFICO
- Universidad Nacional Mayor de San Marcos. (2022). Inconsistencias y ambigüedades en la ley de delitos informáticos ley n° 30096 y su modificatoria ley n° 30171, que imposibilitan su eficaz cumplimiento. <https://hdl.handle.net/20.500.12672/131352>
- Universidad Señor de Sipán. (2021). Modificación legislativa de la ley 30096 de delitos informáticos para su eficacia contra la ciberdelincuencia en la ciudad de Chiclayo. <https://repositorio.uss.edu.pe/handle/20.500.12802/10000>

ANEXOS

Anexo 1.- Evidencia de similitud digital



Página 1 de 47 - Portada

Identificador de la entrega: trn:oid::1:3409847395

JOSÉ CARLOS ADUVIRI FLORES

ANÁLISIS CRÍTICO DE LA REGULACIÓN DE LOS DELITOS INFORMÁTICOS EN EL CÓDIGO PENAL PERUANO

- Titulos
- REVISION 2025
- Universidad Peruana de Ciencias e Informatica

Detalles del documento

Identificador de la entrega
trn:oid::1:3409847395

Fecha de entrega
13 nov 2025, 3:39 p.m. GMT-5

Fecha de descarga
28 nov 2025, 11:32 a.m. GMT-5

Nombre del archivo
IENCIA_PROFESIONAL_DERECHO_29-10-2025- JOSE_ADUVIRI_FLORES-.docx

Tamaño del archivo
68.6 KB

43 páginas

7094 palabras

46.639 caracteres



Página 1 de 47 - Portada

Identificador de la entrega: trn:oid::1:3409847395




11% Similitud general

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

Filtrado desde el informe

- Bibliografía
- Texto citado

Fuentes principales

- 12%  Fuentes de Internet
- 6%  Publicaciones
- 7%  Trabajos entregados (trabajos del estudiante)

Marcas de integridad

N.º de alertas de integridad para revisión

No se han detectado manipulaciones de texto sospechosas.

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

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

Fuentes principales

- 12% Fuentes de Internet
- 6% Publicaciones
- 7% Trabajos entregados (trabajos del estudiante)

Fuentes principales

Las fuentes con el mayor número de coincidencias dentro de la entrega. Las fuentes superpuestas no se mostrarán.

1	Trabajos del estudiante Universidad Peruana de Ciencias e Informatica	3%
2	Internet hdl.handle.net	3%
3	Internet repositorio.upci.edu.pe	<1%
4	Trabajos del estudiante Universidad Privada Antenor Orrego 2025	<1%
5	Publicación Luis Eduardo Morante Mendoza, Jorge Andrés Safadi Mendoza, Gonzalo Patricio G...	<1%
6	Internet sapientia.ucss.edu.pe	<1%
7	Trabajos del estudiante Universidad Mariano Gálvez de Guatemala	<1%
8	Internet repositorio.ucv.edu.pe	<1%
9	Internet repositorio.unp.edu.pe	<1%
10	Internet repositorio.upla.edu.pe	<1%
11	Trabajos del estudiante Universidad Internacional de la Rioja	<1%

12

Publicación

Jorge Santiago Vallejo Lara, Hillary Patricia Herrera Avilés, Edwin Javier Ortega Ca... <1%

13

Internet

www.itu.int <1%

Anexo 2.- Autorización de publicación en repositorio



FORMULARIO DE AUTORIZACIÓN PARA LA PUBLICACIÓN DE TRABAJO DE INVESTIGACIÓN O TESIS EN EL REPOSITORIO INSTITUCIONAL UPCI

1.- DATOS DEL AUTOR

Apellidos y Nombres: Aduviri Flores Jose Carlos
DNI: 014586693 Correo electrónico: Jozeal1901@gmail.com
Domicilio: M2 M Lot 29 Cjta de Agua SJL
Teléfono fijo: 014586693 Teléfono celular: 976322949

2.- IDENTIFICACIÓN DEL TRABAJO Ó TESIS

Facultad/Escuela: Derecho en Ciencias Políticas
Tipo: Trabajo de Investigación Bachiller () Tesis ()
Título del Trabajo de Investigación / Tesis:
Análisis Crítico de la Regulación de los Delitos
Informáticos en el Código Penal Peruano

3.- OBTENER:

Bachiller () Título () Mg. () Dr. () PhD. ()

4. AUTORIZACIÓN DE PUBLICACIÓN EN VERSIÓN ELECTRÓNICA

Por la presente declaro que el documento indicado en el ítem 2 es de mi autoría y exclusiva titularidad, ante tal razón autorizo a la Universidad Peruana Ciencias e Informática para publicar la versión electrónica en su Repositorio Institucional (<http://repositorio.upci.edu.pe>), según lo estipulado en el Decreto Legislativo 822, Ley sobre Derecho de Autor, Art.23 y Art.33.

Autorizo la publicación de mi tesis (marque con una X):

- () Sí, autorizo el depósito y publicación total.
() No, autorizo el depósito ni su publicación.

Como constancia firmo el presente documento en la ciudad de Lima, a los 13 días del mes de Noviembre de 2025.


Firma

